UNIVERSITI MALAYA

SARJANA MUDA SAINS KOMPUTER DENGAN KEPUJIAN

SYAIFUL ANNUAR BIN OMAR

WEK 020243

SECURED EMAIL USING STEGANOGRAPHY

PENYELIA

PUAN FAZIDAH BTE OTHMAN

MODERATOR

EN. NOR BADRUL ANUAR BIN JUMA'AT

PROJEK ILMIAH TAHAP AKHIR

SESI 2004 / 2005

ABSTRAK

Bagi memenuhi keperluan dan syarat bergraduasi yang telah ditetapkan oleh FSKTM, saya telah memilih *Secured Email Using Steganography* sebagai tajuk Latihan Ilmiah saya. Sepanjang tempoh Latihan Ilmiah tersebut, saya dan seorang lagi rakan saya telah memilih tajuk yang sama di bawah selian Puan Fazidah Bte Othman.

Tajuk ini telah dipecahkan kepada dua modul utama iaitu modul pelayan emel (*email server*) dan juga modul sistem *steganography*. Daripada pecahan kedua-dua modul ini, saya telah memilih modul yang kedua iaitu sistem *steganography* sebagai tajuk latihan ilmiah saya. Sistem *steganography* adalah merupakan sistem keselamatan data yang kini semakin popular dikalangan pengguna siber. Ini dapat dibuktikan melalui wujudnya pelbagai sistem yang berasaskan *steganography*.

Sistem *steganography* yang dibangunkan merangkumi dua pecahan modul iaitu modul penyembunyian teks atau fail dan modul pembacaan teks atau fail. Kedua-dua modul ini dibangunkan mengikut peringkat demi peringkat. Setiap modul mempunyai empat sub-modul lain sebagai menepati keperluan pengguna. Modul penyembunyian teks atau fail mengandungi sub-modul membuka fail imej, pemilihan teks atau fail, pengesahan kata laluan, penyembunyian teks atau fail dan penyimpanan. Modul pembacaan teks atau fail pula mengandungi sub-modul membuka fail imej, pengesahan kata laluan, pemisahan data daripada imej dan paparan teks atau penyimpanan fail. Pembangunan sistem ini dibangunkan menggunakan sepenuhnya perisian *Microsoft Visual Basic 6.0*.

PENGHARGAAN

Alhamdulillah, bersyukur saya ke hadrat Allah kerana dengan limpah kurnia dan restu darinya, akhirnya saya selesai menyiapkan laporan Latihan Ilmiah I (WXES 3181) dan Latihan Ilmiah II (WXES 3182) dari 22 Jun 2004 sehingga 04 Mac 2005 di bawah selian Puan Fazidah Bte Othman.

Terlebih dahulu, ribuan terima kasih diucapkan kepada Puan Fazidah Bte Othman selaku penyelia latihan ilmiah saya kerana sudi menerima saya sebagai salah seorang pelajar di bawah selian beliau. Segala bantuan, pertolongan dan penerangan yang diberikan sewaktu menyiapkan laporan Latihan Ilmiah I dan pembangunan sistem *steganography* adalah sangat-sangat dihargai. Pengetahuan yang diberikan bukan sahaja untuk dipraktikkan pada waktu ini, tetapi juga di alam pekerjaan. Kepercayaan dan peluang yang diberikan untuk menyiapkan laporan dan sistem *steganography* adalah amat dihargai. Dengan bantuan dan dorongan beliau, laporan Latihan Ilmiah I dan sistem *steganography* berjaya disiapkan dan dibangunkan. Semoga bantuan dan kerjasama yang diberikan akan terus berkekalan di masa-masa akan datang.

Disamping itu juga, ribuan terima kasih diucapkan kepada Encik Nor Badrul Anuar Bin Juma'at yang bertindak selaku moderator kerana turut bersama-sama berkongsi pendapat dan idea untuk dimuatkan ke dalam sistem yang dibangunkan ini.

Tidak lupa juga kepada semua pensyarah FSKTM yang banyak memberi didikan dan pengetahuan kepada saya sepanjang saya berada di FSKTM. Segalanya adalah amat berharga dan sebahagiannya telah saya gunakan untuk dijadikan rujukan dan panduan semasa menyiapkan laporan Latihan Ilmiah I dan membangunkan

sistem *steganography*. Tanpa mereka semua, pengetahuan yang ada mungkin tidak dapat diaplikasikan ke dalam sistem saya ini.

Akhir sekali, terima kasih diucapkan kepada rakan seperjuangan saya yang sama-sama memberi pendapat dan idea untuk membangunkan sistem *steganography* ini terutama sekali Encik Razlan Salleh dan Cik Mazidah Mat Isa yang juga bertindak selaku penguji utama sistem ini. Pendapat dan pembelajaran yang diberikan akan disimpan dan digunakan bukan sahaja pada ketika ini tetapi sampai bila-bila. Terima kasih sekali lagi.

ISI KANDUNGAN

SENARAI RAJAH

SENARAI JADUAL

BAB 1
PENGENALAN PROJEK

BAB 1

PENGENALAN PROJEK

1.1 LATAR BELAKANG PROJEK

Steganography merupakan satu cara berkomunikasi yang selamat di mana komunikasi antara dua pihak dapat dijalankan dengan cara penyembunyian data. Data yang disembunyikan termasuklah dari segi teks atau fail. *Steganography* selalunya dikaitkan dengan persamaan kriptografi. Walaupun mempunyai persamaan, teknik yang digunakan adalah berlainan dan *steganography* mempunyai kelebihan tersendiri yang tidak terdapat pada kriptografi.

Sistem *steganography* yang akan dibangunkan ini adalah bertujuan untuk mengaplikasikan secara amnya mengenai apa yang dimaksudkan dengan *steganography*. Pengguna akan dapat berkomunikasi dengan lebih selamat melalui penggunaan sistem ini terutama sekali melalui emel. Melalui sistem ini juga, tiada siapa akan mengetahui tentang data yang tersembunyi disebalik fail lain dan sukar untuk dikenal pasti. Dengan ini, pengguna akan dapat membaca data yang dihantar tanpa sebarang pencerobohan.

Secara amnya, terdapat tiga kaedah utama dalam proses penyembunyian data melalui *steganography*, iaitu :-

- melalui teks
- melalui imej (bergantung kepada format imej)
- melalui audio (bergantung kepada format audio)

Ketiga-tiga teknik di atas mempunyai kebaikan dan kelebihan yang tersendiri yang akan diterangkan dalam bab kajian literasi. Bagi sistem *steganography* yang akan dibangunkan ini, teknik kedua iaitu teknik penyembunyian data melalui imej akan digunakan. Teknik ini lebih senang dipraktikan dan diaplikasikan berbanding dua teknik lain yang dinyatakan. Pengguna juga akan lebih senang memahami teknik dan sistem yang akan dibangunkan ini.

Sistem ini akan meliputi dua modul iaitu modul penyembunyiaan data melalui imej sehingga ke modul pembacaan data. Kedua-dua modul ini merupakan modul utama dalam sistem yang akan dibangunkan ini. Terdapat juga beberapa modul kecil dalam kedua-dua modul utama ini seperti pengesahan kata laluan, penyembunyian data, membaca data, penyimpanan fail dan sebagainya.

Sistem yang akan dibangunkan ini mempunyai ciri-ciri yang tertentu yang tidak terdapat pada sistem yang sedia ada. Selain itu, sistem ini dapat membaiki kelemahan-kelemahan yang terdapat dalam sistem yang sedia ada seperti kriptografi. Sehubungan itu, sistem ini akan menjadi lebih penting dan bermanfaat sejajar dengan revolusi alam siber yang lebih mementingkan keselamatan data daripada dicerobohi.

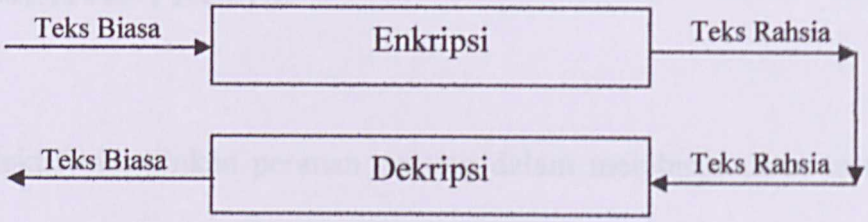
1.2 MOTIVASI PROJEK

Motivasi projek bagi sistem *steganography* ini adalah berpandukan kepada kelemahan pada sistem keselamatan yang sedia ada dan objektif utama sistem *steganography*. Sistem yang akan dibangunkan ini mempunyai kelebihan yang tersendiri untuk diaplikasikan berbanding dengan sistem-sistem yang sedia ada. Dengan kewujudan sistem ini, pelbagai masalah pencerobohan terhadap data yang dihantar dapat diatasi dengan segera. Sistem ini akan memperbaiki segala kelemahan atau masalah sistem yang sedia ada daripada modul penyembunyian data disebalik imej sehingga modul pembacaan data oleh penerima.

1.2.1 KELEMAHAN SISTEM SEDIA ADA

Kebanyakan sistem keselamatan yang ada sekarang adalah menggunakan teknik kriptografi. Teknik kriptografi merupakan salah satu teknik keselamatan yang popular untuk diaplikasikan. Namun demikian, sehingga ke hari ini, pelbagai masalah sering timbul dalam penggunaannya sebagai sistem keselamatan. Kelemahan-kelemahan tersebut ialah :-

- Kebanyakan kekunci awam yang digunakan terlalu komplek untuk diaplikasikan dalam teknik ini.
- Kebanyakan kekunci awam yang digunakan boleh dikenal pasti oleh penceroboh untuk melakukan enkripsi data dengan mudah.



Rajah 1.1 : Gambaran secara am proses kriptografi dilaksanakan

1.2.2 PENYELESAIAN DAN KELEBIHAN *STEGANOGRAPHY*

Salah satu penyelesaian bagi masalah sistem kriptografi adalah dengan wujudnya sistem atau teknik *steganography*. Walaupun sistem atau teknik ini tidak banyak digunakan dan diaplikasikan pada ketika ini, tetapi steganography tetap menjadi satu sistem atau teknik yang lebih selamat berdasarkan kepada ciri-ciri yang dimiliki olehnya. Ini merupakan kelebihan yang dimiliki oleh sistem *steganography*. Kelebihan-kelebihan lain ialah :-

- penghantaran maklumat atau fail kepada penerima tidak dapat dikesan dengan mudah oleh orang lain seperti mana sistem kriptografi yang lebih senang dicerobohi.
- maklumat atau fail yang disembunyikan boleh dihantar dengan pelbagai format atau cara yang tidak boleh dikesan atau dibaca oleh pengguna lain.

1.3 OBJEKTIF PROJEK

Objektif memainkan peranan penting dalam membangunkan sesuatu projek atau sistem. Objektif-objektif ini akan menentukan matlamat sebenar keseluruhan projek atau sistem yang akan dibangunkan. Oleh sebab itu, dalam membangunkan sistem *steganography* ini, terdapat lima objektif utama, iaitu :-

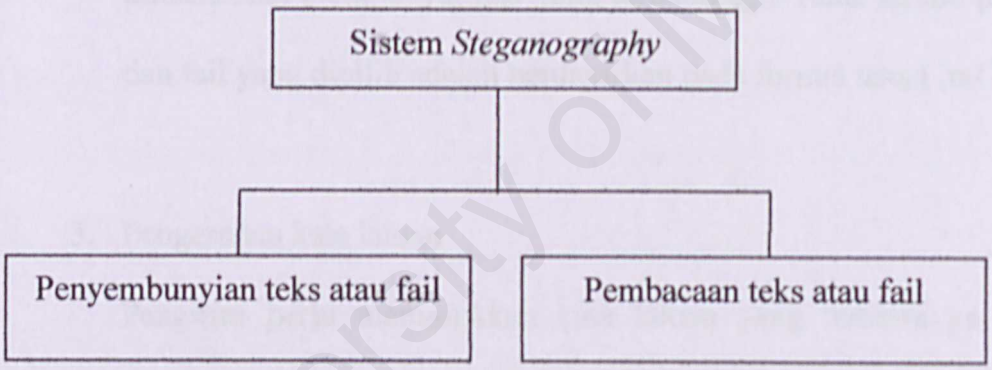
- Untuk membangunkan satu sistem yang lebih selamat dan juga mempunyai ciri-ciri keselamatan yang lebih baik yang boleh menggantikan sistem-sistem penyembunyian data yang lain.
- Untuk mengurangkan masalah-masalah pencerobohan yang sering berlaku kepada data (teks atau fail) yang dihantar melalui emel.
- Untuk mewujudkan satu komunikasi yang lebih selamat terutama sekali melalui emel dikalangan pengguna-pengguna yang dikenali.
- Untuk membangunkan satu sistem yang lebih mesra pengguna, mudah dilaksanakan dan digunakan serta diaplikasikan.
- Untuk menggalakkan pengguna-pengguna lebih kerap berkomunikasi melalui emel disebabkan adanya sistem *steganography* berbanding dengan medium komunikasi yang lain.

1.4 SKOP PROJEK

Bagi sistem *steganography* yang akan dibangunkan ini, terdapat dua modul utama, iaitu :-

- modul penyembunyian teks atau fail
- modul pembacaan teks atau fail

Kedua-dua modul utama ini akan dibahagikan kepada beberapa modul kecil agar setiap modul dapat dilaksanakan dengan mudah.



Rajah 1.2 : Modul Sistem *Steganography*

1.4.1 MODUL PENYEMBUNYIAN TEKS ATAU FAIL

Modul penyembunyian teks atau fail ini direka khas untuk pengirim menyembunyikan teks atau fail sebelum dihantar kepada penerima melalui emel. Modul ini merangkumi beberapa modul kecil agar perlaksanaan penyembunyian teks atau fail dapat dilakukan oleh pengirim dengan lebih mudah. Modul-modul ini boleh

dikatakan sebagai proses yang perlu dilalui dalam modul tersebut. Setiap modul-modul kecil ini mempunyai peranan tertentu. Modul-modul kecil tersebut ialah :-

1. Membuka fail imej

   Pembukaan fail imej digunakan untuk memilih imej yang diperlukan bagi tujuan menyembunyikan teks atau fail disebaliknya. Imej yang dipilih adalah berdasarkan pada format bitmap (.bmp).

2. Pemilihan teks atau fail

   Pengirim akan memasukkan maklumat yang berbentuk teks atau memilih fail untuk disembunyikan disebalik imej. Teks yang dimasukkan mempunyai had yang tertentu agar tidak terlalu panjang dan fail yang dipilih adalah berdasarkan pada format teks (.txt).

3. Pengesahan kata laluan

   Pengirim perlu memasukkan kata laluan yang tertentu ke dalam sistem. Ini penting kerana, kata laluan yang digunakan oleh pengirim akan turut digunakan oleh penerima untuk membaca teks atau fail yang dihantar. Kata laluan ini hanya diketahui oleh pengirim dan penerima sahaja agar setiap teks atau fail yang dihantar tidak dapat dibaca oleh orang lain.

4. Penyembunyian teks atau fail

   Proses penyembunyian dilaksanakan berdasarkan teks yang dimasukkan atau fail yang dipilih oleh pengirim.

5. Penyimpanan

   Selepas penyembunyian disebalik imej berjaya dilakukan, imej tersebut akan disimpan sebagai fail imej yang baru atau menggantikan fail imej yang lama. Kemudian, pengirim akan menggunakan fail imej ini untuk dihantar kepada penerima melalui emel.

1.4.2 MODUL PEMBACAAN TEKS ATAU FAIL

Modul ini pula direka khas kepada penerima untuk membaca teks atau fail yang disembunyikan yang diterima daripada pengirim. Penerima akan membaca data yang diterima melalui modul ini. Modul ini mempunyai beberapa modul kecil yang sama seperti modul penyembunyian teks atau fail. Modul-modul kecil tersebut ialah :-

1. Membuka fail imej

   Fail imej yang diterima daripada pengirim akan dibuka untuk membaca teks atau fail dalam proses yang berikutnya.

2. Pengesahan kata laluan

   Penerima perlu memasukkan kata laluan yang sama dengan kata laluan pengirim agar dapat membaca teks atau fail disebalik imej. Kata laluan yang salah akan menyebabkan penerima tidak boleh membaca teks atau fail yang disembunyikan.

3. Pemisahan data daripada imej

   Selepas fail imej dipilih, pemisahan data daripada imej akan dilakukan. Data akan dipisahkan daripada imej agar penerima boleh membaca data yang tersembunyi disebalik imej tersebut.

4. Paparan teks atau penyimpanan fail

   Teks yang tersembunyi akan dipaparkan atau fail yang didapati akan disimpan terlebih dahulu sebelum dapat membacanya.

1.5 SASARAN PENGGUNA

Sasaran utama pengguna bagi sistem ini adalah dikalangan kakitangan kerajaan dan swasta di Malaysia. Ini termasuklah sektor-sektor kerajaan seperti Kementerian Pertahanan, Kementerian Pendidikan dan sebagainya. Ini kerana, mereka mempunyai maklumat sulit yang perlu dirahsiakan daripada pengguna-pengguna lain. Melalui sistem ini, segala maklumat sulit yang dihantar tidak dapat diceroboh oleh pengguna-pengguna lain tanpa keizinan mereka. Dengan sistem ini, segala maklumat sulit dapat dilindungi daripada pengguna-pengguna lain. Oleh sebab itu, penggunaan sistem ini adalah bertepatan dan bersesuaian untuk kakitangan kerajaan dan swasta demi menjamin keselamatan maklumat sulit mereka.

1.6 HASIL YANG DIJANGKAKAN

Sistem *steganography* ini dibangunkan dengan merangkumi kesemua kriteria seperti yang telah dinyatakan dalam bahagian skop dan objektif projek dengan menggunakan sumber dan peralatan perisian yang bersesuaian. Ini penting bagi menghasilkan satu sistem yang baik dan berkualiti di akhir fasa pembangunan sistem. Bagi sistem *steganography* ini, pelbagai hasil yang dijangkakan, iaitu :-

1. Mesra pengguna

   Sistem *steganography* yang dibangunkan adalah satu sistem yang lebih mesra pengguna yang membolehkan pengguna berinteraksi dengan sistem. Selain itu, pengguna akan lebih senang memahami penggunaan dan perjalanan sistem dengan lebih cepat. Sebarang masalah lebih senang diatasi dengan sistem yang lebih mesra penguna.

2. Mudah dan konsisten

   Sistem ini dikatakan mudah kerana menggunakan aturcara pengekodan yang mudah dan tidak kompleks. Sistem ini juga senang digunakan berbanding dengan sistem-sistem yang lain. Ini juga akan memudahkan penyelenggaran sistem seperti membaik pulih semula sistem yang telah dibangunkan.

3. Kawalan capaian yang ketat

   Kawalan capaian yang ketat penting dalam sesuatu sistem. Hanya pengguna yang berdaftar iaitu pengguna yang mengetahui kata laluan pengirim sahaja akan dapat membaca maklumat atau fail yang dihantar.

4. Kebolehan kepercayaan yang tinggi

   Sistem ini boleh dipercayai kerana mempunyai ciri-ciri keselamatan yang baik untuk mengelakkan sebarang pencerobohan terhadap maklumat atau fail yang dihantar seperti kata laluan dan proses penyembunyian data yang digunakan.

1.7 HAD SISTEM

Terdapat enam kekangan atau had sistem dalam sistem *steganography* yang dibangunkan, iaitu :-

- Sistem *steganography* yang dibangunkan adalah bukan untuk jangka masa yang panjang.
- Imej yang digunakan sebagai pelindung objek hanyalah imej yang berfomat bitmap 24-bit sahaja.
- Teks yang hendak disembunyikan adalah terhad iaitu sebanyak 2000 huruf.
- Fail yang digunakan untuk disembunyikan hanyalah fail berformat teks iaitu .txt sahaja.
- Fail teks yang mengandungi jumlah perkataan yang besar dan saiz fail yang besar akan menyebabkan masa tindak balas sistem menjadi lambat. Ini kerana, setiap huruf akan disembunyikan pada setiap bit imej.

- Saiz imej bitmap 24-bit yang digunakan sebagai pelindung objek tidak boleh melebihi 1 MB bagi mengelakkan proses penghantaran emel menjadi lambat.
- Hanya pengguna yang mempunyai sistem yang seumpama dengan sistem *steganography* boleh membaca teks atau fail yang disembunyikan disebalik imej.

1.8 PENJADUALAN PROJEK

Bagi menghasilkan sesuatu sistem yang baik, penjadualan projek haruslah bersesuaian dan tersusun. Ini penting agar segala aktiviti dan proses kerja dapat disiapkan dalam tempoh masa yang ditetapkan. Penjadualan projek akan menerangkan segala aktiviti yang dilakukan bagi setiap fasa dalam kitaran pembangunan sistem. Penjadualan projek juga akan menunjukan kesinambungan antara satu fasa dengan fasa yang lain serta menjadi panduan dalam mencapai matlamat utama bagi setiap fasa yang dilalui. Penjadualan projek bagi sistem *steganography* adalah seperti berikut :-

1. Pengenalan projek
    - segala maklumat dikumpul mengenai projek yang akan dibangunkan
    - secara ringkas dan menyeluruh mengenai projek yang akan dibangunkan

2. Kajian literasi

   - mengumpul maklumat yang berkaitan dengan sistem *steganography*
   - melakukan kajian mengenai masalah secara am dan terperinci mengenai *steganography*
   - mendalami segala maklumat yang dikumpul dalam fasa pertama

3. Analisa sistem

   - segala maklumat dalam fasa kedua diguna pakai semula
   - memilih dan menentukan model pembangunan yang akan digunakan
   - mendalami objektif sistem yang ditentukan dalam fasa pertama
   - menganalisa segala keperluan sistem yang akan dibangunkan

4. Rekabentuk sistem

   - merekabentuk skrin utama sistem
   - merekabentuk setiap paparan dalam sistem
   - merekabentuk carta alir sistem

5. Pembangunan sistem

   - berhubung kait dengan fasa rekabentuk sistem
   - mencipta arahan-arahan dan fungsi-fungsi utama sistem
   - memasukkan arahan-arahan dan fungsi-fungsi tersebut ke dalam sistem

6. Pengujian sistem

   - setiap fasa akan diuji dari semasa ke semasa
   - keseluruhan sistem akan diuji setelah selesai fasa pembangunan sistem
   - ditentukan dengan perkakasan sistem mengikut kesesuaiannya
   -

7. Penilaian sistem

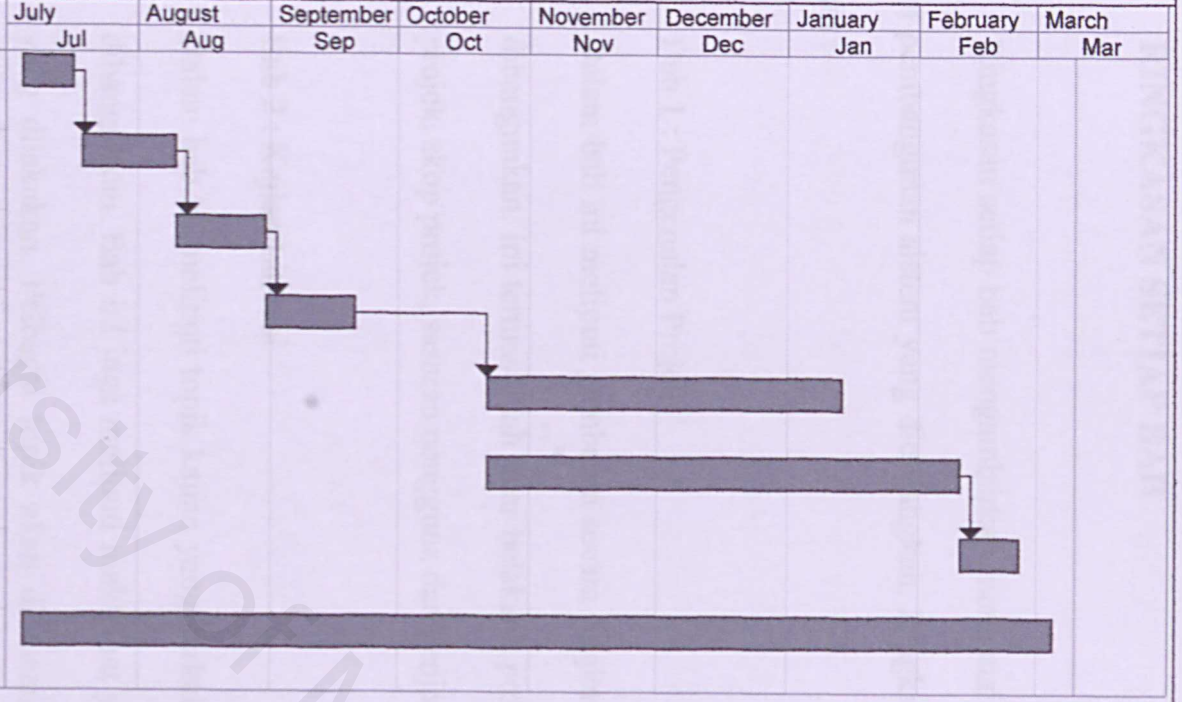
   - melakukan penilaian sistem mengikut kriteria iaitu kekuatan sistem, kekangan atau had sistem dan perancangan masa hadapan sistem.
   - masalah dan penyelesaian pada pembangun sistem dan cadangan yang diberikan.

8. Dokumentasi

   - menyediakan manual pengguna bagi sistem
   - menyediakan format persembahan untuk VIVA I dan VIVA II
   - menyiapkan laporan untuk dihantar

Jadual 1.1 : Jadual perjalanan bagi pembangunan sistem *steganography*.

ID	Task Name	Duration	Start	Finish
1	Pengenalan Projek	10 days	Mon 7/5/04	Fri 7/16/04
2	Kajian Literasi	16 days	Mon 7/19/04	Mon 8/9/04
3	Analisa Sistem	15 days	Tue 8/10/04	Mon 8/30/04
4	Rekabentuk Sistem	15 days	Tue 8/31/04	Mon 9/20/04
5	Perlaksanaan Sistem	60 days	Fri 10/22/04	Thu 1/13/05
6	Pengujian Sistem	80 days	Fri 10/22/04	Thu 2/10/05
7	Penilaian Sistem	10 days	Fri 2/11/05	Thu 2/24/05
8	Dokumentasi	175 days	Mon 7/5/04	Fri 3/4/05



1.9 RINGKASAN SETIAP BAB

Ringkasan setiap bab mengambarkan mengenai fasa-fasa utama yang terlibat dalam pembangunan sistem yang dicadangkan. Ringkasan setiap bab adalah seperti berikut :-

Bab 1 : Pengenalan Projek

Dalam bab ini meliputi gambaran secara ringkas mengenai projek yang akan dibangunkan. Ini termasuklah latar belakang projek, motivasi projek, objektif projek, skop projek, sasaran pengguna dan penjadualan projek.

Bab 2 : Kajian Literasi

Dalam bab ini meliputi topik kajian yang berkaitan dengan sistem yang akan dibangunkan. Bab ini juga meliputi maklumat yang didapati daripada kajian yang dilakukan. Pelbagai topik akan dibincangkan dalam bab ini seperti senibina sistem dan perkakasan sistem.

Bab 3 : Methodologi

Bab ini akan memfokuskan pada model pembangunan dan kaedah yang akan digunakan. Bab ini juga menerangkan mengenai bahasa dan methodologi yang dipilih. Selain itu, fasa pertama akan dianalisa dalam bab ini.

Bab 4 : Analisa Sistem

Bab ini akan memfokuskan kepada penganalisaan kehendak projek dan fungsi sebenar projek. Bab ini juga akan menerangkan bagaimana kesemua

kehendak yang ditetapkan pada fasa pertama ditepati atau tidak. Segala analisa yang dilakukan adalah berdasarkan kepada perkakasan dan perisian yang sesuai, struktur carta dan juga model pembangunan yang digunakan.

Bab 5 : Rekabentuk Sistem

Bab ini akan menerangkan struktur rekabentuk bagi setiap antaramuka yang digunakan termasuklah skrin utama dan paparan output. Segala grafik yang bersesuaian juga akan dipilih untuk dimasukkan ke dalam sistem. Selain itu, bab ini turut memfokuskan pada aliran data sistem dan modul sistem *steganography*.

BAB 2
KAJIAN LITERASI

BAB 2

KAJIAN LITERASI

2.1 KAJIAN LITERASI SECARA AM

Bagi memastikan setiap projek berjalan dengan lancar dan teliti, pembangun sistem haruslah membuat beberapa kajian sebelum melangkah ke proses seterusnya. Ini penting kerana setiap kajian yang dilakukan adalah bersamaan dengan proses mendapatkan dan mengumpulkan maklumat-maklumat yang berkaitan dengan sistem yang akan dibangunkan. Selain itu, proses ini juga dapat memberikan idea dan maklumat kepada pembangun sistem mengenai bagaimana sistem tersebut dapat dibangunkan disamping memilih teknik yang harus digunakan serta teknologi yang bagaimana harus diaplikasikan dalam membangunkan sistem tersebut. Kajian ini akan meliputi segala kaedah pencarian dan analisis maklumat yang berkaitan.

Kajian literasi ini juga penting dalam membantu pembangun sistem untuk mengenal pasti apa sebenarnya kehendak dan tujuan sistem tersebut (*system requirements*). Sehubungan itu, kemungkinan pembangun sistem boleh menambah beberapa ciri baru yang diperlukan pada sistem dan mengetahui cara-cara untuk mengatasi masalah yang akan muncul sebelum atau selepas sistem dibangunkan. Kesemua ini akan memberikan pengalaman dan pengetahuan baru kepada pembangun sistem terutama sekali kepada pembangun sistem yang baru.

2.1.1 KAEDAH PENCARIAN MAKLUMAT

Terdapat pelbagai kaedah dalam proses pencarian dan pengumpulan maklumat. Kesemua kaedah ini diperlukan dalam memastikan maklumat yang didapati adalah boleh dipercayai untuk diaplikasikan kepada sistem. Setiap pembangun sistem harus memilih kaedah pencarian yang betul agar maklumat yang didapati lebih mudah dan tidak memakan masa yang panjang.

Bagi sistem *steganography* ini, tiga kaedah utama yang digunakan dalam pencarian maklumat, iaitu :-

- Berbincang dengan penyelia projek
- Pencarian maklumat melalui internet
- Pemerhatian dan temubual secara tidak rasmi

2.1.1.1 Berbincang Dengan Penyelia Projek

Kaedah ini merupakan kaedah utama yang digunakan. Kaedah ini meliputi dari awal pembangunan sistem sehingga tamat pembangunan sistem. Tujuan utama kaedah ini adalah untuk memastikan setiap objektif, skop dan misi yang sudah dimaklumkan sentiasa diikuti dan ditepati. Disamping itu juga, penyelia akan memberi maklum balas dan idea bagaimana untuk membangunkan sistem dan untuk membuat keputusan secara tepat berdasarkan sistem yang dibangunkan. Sebahagian yang didapati daripada penyelia akan digunakan dalam menentukan ciri-ciri yang perlu dimuatkan ke dalam sistem seperti bahasa pengaturcaraan dan platform yang sesuai dengan sistem *steganography*. Kaedah ini adalah yang paling pantas untuk

mendapatkan maklumat dan idea yang bersesuaian serta dapat memastikan perjalanan pembangunan sistem mengikut apa yang telah dirancangkan pada awalnya.

2.1.1.2 Pencarian Maklumat Melalui Internet

Pencarian maklumat melalui internet adalah kaedah kedua yang digunakan. Ini termasuklah proses memuat turun servis dan dokumentasi yang berkaitan dengan sistem *steganography*. Melalui pembacaan daripada laman web tersebut dapat memberi pelbagai maklumat yang berkaitan dengan sistem *steganography* ini. Sekaligus dapat membantu mendapatkan maklumat dengan cepat, tepat dan mudah. Kaedah ini merupakan kaedah yang paling pantas berbanding antara tiga kaedah yang diutamakan.

2.1.1.3 Pemerhatian dan Temubual Secara Tidak Rasmi

Pemerhatian perlu dilakukan seiring ketika sistem dibangunkan. Ini penting agar sistem yang dibangunkan meliputi ciri-ciri yang terkini dan bersesuaian. Pemerhatian dijalankan untuk mendapatkan maklumat bagaimana sesuatu perisian digunakan, bagaimana untuk mengaplikasikan bahasa pengaturcaraan yang bersesuaian dan banyak lagi perkara-perkara yang berkaitan. Justeru itu sesuatu sistem dapat dibangunkan mengikut kesesuaian semasa dan senang dipelajari. Pemerhatian juga dapat mendedahkan mengenai wujudnya sistem-sistem *steganography* yang terdahulu. Daripada pemerhatian ini, dapat memberitahu mengenai

kelemahan dan kekuatan sistem yang sedia ada dan bagaimana untuk membangunkan semula sistem dengan ciri-ciri yang lebih baik agar segala kelemahan dapat diatasi. Temubual secara tidak rasmi ini meliputi pelbagai pihak termasuklah rakan-rakan sendiri. Tujuan utamanya adalah untuk mendapatkan maklum balas mengenai sistem *steganography* seperti peralatan yang akan digunakan dan tunjuk ajar dalam penggunaan sesuatu perisian baru.

2.2 PENGGUNAAN EMEL SEBAGAI MEDIUM UTAMA

Pada masa ini, emel merupakan medium komunikasi utama dalam konteks perhubungan antara satu pihak dengan pihak yang lain. Emel banyak digunakan untuk berkomunikasi secara jarak jauh bagi menggantikan surat, faks dan telefon pada suatu ketika dahulu sekaligus dapat mengurangkan kos perhubungan. Emel bukan sahaja dipelopori oleh golongan dewasa bahkan turut dipelopori oleh golongan pelajar, remaja dan warga emas. Ini dapat dibuktikan daripada populariti emel sebagai medium utama untuk berkomunikasi.

Emel atau mel elektronik adalah istilah yang diberikan kepada mesej elektronik yang biasanya digunakan dalam bentuk mesej teks yang mudah ditaip pada sistem komputer dan dihantar melalui rangkaian komputer kepada pengguna-pengguna lain yang boleh membaca emel tersebut. Pada awalnya emel hanya meliputi dalam bentuk mesej teks, tetapi pelbagai ciri-ciri tambahan ditambah agar emel yang dihantar lebih menarik dan boleh mengandungi gambar dan fail tertentu.

Oleh sebab itu, emel lebih mudah mendapat perhatian daripada medium-medium komunikasi yang lain.

Sistem emel terbahagi kepada dua bahagian iaitu penghantaran dan penerimaan. Kedua-dua sistem ini penting dalam menjayakan perlaksanaan emel. Konsep penghantaran dan penerimaan ini pada awalnya adalah terhad penggunaannya dimana hanya boleh diaplikasikan di kawasan pejabat, kawasan yang mempunyai perisian emel yang sama dan kawasan yang mempunyai rangkaian yang sama. Kini, penggunaan emel tidak terhad seperti dahulu. Emel sudah boleh dihantar keluar melalui internet dan tiada had kawasan diperuntukkan. Pelbagai syarikat sudah banyak mewujudkan emel mereka sendiri dan pengguna boleh mendaftar mengikut kehendak mereka sendiri. Antara nama-nama besar yang boleh dikaitkan dengan emel ialah *Hotmail* dan *Yahoo*. Kedua-dua syarikat ini adalah pelopor terbesar dalam emel.

Perkembangan emel dari semasa ke semasa menyebabkan pengguna lebih selesa untuk berkomunikasi menggunakan emel sebagai medium utama menggantikan telefon yang suatu ketika dahulu lebih mendapat perhatian. Selain perkembangan secara mendadak, emel juga mendapat perhatian disebabkan murah, mudah untuk menggunakannya dan tidak dikenakan sebarang kos pembayaran atas servis yang digunakan. Disebabkan penggunaan emel yang begitu meluas, pengguna lebih gemar menghantar maklumat rahsia melalui emel tanpa memikirkan sebarang risiko yang mungkin berlaku pada maklumat tersebut. Pencerobohan yang berlaku ketika ini adalah bersamaan dengan pengguna yang menggunakan emel pada hari ini. Oleh sebab itu, sistem *steganography* perlu diwujudkan bagi mengatasi masalah sedemikian. Sistem ini bukan sahaja diaplikasikan pada emel yang mengandungi

maklumat rahsia tetapi juga pada emel biasa agar masalah pencerobohan dapat diatasi.

2.2.1 KEBAIKAN EMEL

1. Emel menjadi tulang belakang dalam perhubungan dan komunikasi.
   - penghantaran mesej elektronik dapat dihantar ke seluruh dunia dengan lebih cepat.
   - kos penghantaran emel lebih murah atau percuma berbanding dengan medium komunikasi yang lain.
2. Emel lebih baik daripada sistem pos yang sedia ada.
   - penghantaran yang lebih cepat.
   - penghantaran terus kepada penerima.
3. Emel yang dihantar mempunyai rekod yang tersendiri dimana mesej yang dihantar boleh disimpan dan pengirim boleh mengetahui samada mesej yang dihantar mempunyai alamat yang betul atau tidak.
4. Penerima boleh membaca emel yang diterima dimana sahaja mereka berada melalui rangkaian internet.
5. Emel boleh dihantar ke serata dunia tanpa perlu bergerak ke mana-mana dan hanya menggunakan sistem komputer sahaja.
6. Emel tidak memerlukan kertas dan ruang simpanan pada cakera keras, disket dan seumpamanya.

2.3 KRIPTOGRAFI

Kaedah kriptografi adalah kaedah yang sering menjadi perhatian dan sering digunakan sebelum wujudnya kaedah penyembunyian maklumat dan data. Kriptografi yang bermaksud menulis secara rahsia dicipta bertujuan untuk menghalang pengguna yang tidak mempunyai hak dalam membaca mesej yang dihantar kepada penerima yang sebenarnya.

Sistem kriptografi terdiri daripada empat jenis perlindungan dalam memastikan kualiti mesej asal dijaga, iaitu :-

- Rahsia - melindungi daripada penceroboh menyekat atau menghalang mesej yang dihantar.
- Pengesahan - memastikan agar pengirim adalah yang dikenali.
- Keaslian - memastikan kandungan mesej tidak diubah sebelum diterima oleh penerima.
- Perlindungan - memastikan mesej yang telah diubah oleh penceroboh dan menghantarnya semula tidak diterima oleh penerima asal.

2.3.1 KEKUNCI ENKRIPSI

Teks biasa :-

Mesej asal yang akan dihantar kepada penerima dikenali sebagai teks biasa dan tidak terhad kepada mesej teks sahaja. Teks biasa juga boleh terdiri daripada grafik, suara dan sebagainya.

Enkripsi dan teks rahsia :-

Enkripsi adalah satu proses matematik yang digunakan untuk menukarkan teks biasa kepada sesuatu yang dikenali sebagai teks rahsia. Teks rahsia pula terjadi hasil daripada proses enkripsi yang terdiri daripada rentetan nombor sifar dan satu secara rawak dimana sesiapa tidak dapat membaca kandungan asal teks biasa terutama mereka yang ingin mengubahsuai atau menyekat mesej tersebut.

Dekripsi :-

Dekripsi adalah proses untuk menukarkan mesej teks rasia kepada mesej asal teks biasa. Apabila penerima yang sebenar menerima mesej teks rahsia daripada pengirim, penerima boleh melakukan proses dekripsi ke atas mesej teks rahsia iaitu melakukan proses matematik untuk menghasilkan semula mesej asal teks biasa.

2.3.2 KAEDAH ENKRIPSI

Proses enkripsi terbahagi kepada dua bahagian, iaitu :-

- Algoritma matematik
- Kunci (*string of bits*)

  - kunci yang berbeza akan menghasilkan teks rahsia yang berlainan walaupun menggunakan kaedah yang sama.

2.3.3 KEKUNCI ENKRIPSI BERSIMETRI

Kekunci enkripsi bersimetri adalah kaedah yang menggunakan hanya satu kekunci untuk melakukan proses enkripsi dan juga proses dekripsi. Kekunci enkripsi dan kekunci dekripsi adalah sama. Contoh-contoh kekunci enkripsi bersimetri ialah :-

- Data Encryption Standard (DES)
- DES – Cipher Block Chaining (DES – CBC)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)
- IDEA
- RC4

2.3.4 KEKUNCI ENKRIPSI AWAM

Kekunci enkripsi awam pula adalah kaedah yang menggunakan dua kekunci yang berlainan untuk melakukan proses enkripsi dan dekripsi. Proses enkripsi memerlukan kekunci awam yang dipegang oleh semua pihak manakala proses dekripsi pula memerlukan kekunci rahsia yang disimpan secara rahsia dan tidak diketahui oleh sesiapa. Kaedah ini juga dikenali sebagai kekunci enkripsi asimetri. Contoh-contoh kaedah ini ialah :-

- RSA
- Elliptic Curve Cryptosystem (ECC)

2.3.5 KELEMAHAN

Walaupun kriptografi menjadi perhatian utama untuk melindungi mesej daripada diceroboh oleh pengguna yang tidak mempunyai hak untuk membacanya, terdapat juga kelemahan-kelemahan yang menjadikan kaedah dan sistem ini menimbulkan keraguan kepada setiap pihak untuk menggunakannya. Antara kelemahan-kelemahan kriptografi ialah :-

- Kekunci enkripsi bersimetri
  - Kekunci yang kurang daripada 100 kekunci adalah dikenali sebagai kekunci yang lemah.

- Kekunci enkripsi awam
  - Kekunci awam yang digunakan adalah terlalu komplek untuk diaplikasikan dalam proses enkripsi.
  - Kekunci awam yang digunakan boleh dikenal pasti oleh pengguna lain untuk melakukan proses enkripsi terhadap mesej dengan senang.
  - Kekunci awam hanya boleh digunakan untuk mesej yang pendek.

2.4 PENYEMBUNYIAN MAKLUMAT

Penyembunyian maklumat merupakan satu konsep yang digunakan dalam menjadikan segala data dapat dilindungi dengan selamat tanpa sebarang pencerobohan. Komunikasi menggunakan emel sebagai medium utama adalah komunikasi yang menjadi pilihan ramai pada hari ini. Justeru itu, segala maklumat yang dihantar dan juga diterima perlulah dilindungi daripada berlakunya pencerobohan terhadap emel tersebut. Namun demikian, teknik-teknik penyembunyian maklumat yang sedia ada tidak dapat memastikan segalanya dapat dilindungi dengan selamat. Daripada kajian yang dijalankan sehingga ke hari ini, teknik menyembunyikan maklumat adalah lebih baik daripada teknik-teknik yang lain.

Penyembunyian maklumat mempunyai intipati yang tersendiri yang dapat meningkatkan keselematan maklumat dan keselamatan trafik rangkaian daripada diceroboh oleh pengguna lain. Penyembunyian maklumat ini juga meliputi pelbagai peraturan atau peranan tersembunyi yang menggabungkan :-

- Kriptografi
- Teori komunikasi
- Teori pengekodan
- Isyarat pemampatan
- Teori visual dan audio

Gabungan peraturan-peraturan di atas menyebabkan kaedah penyembunyian maklumat berbeza dengan kaedah sebelum ini yang hanya mempunyai satu atau dua peraturan dan juga hanya melindungi kandungan mesej.

Mengikut sejarah perkembangan penyembunyian maklumat, kaedah ini telah lama diaplikasikan seperti menulis surat menggunakan susu, menggunakan gema di dalam lagu dan menggunakan tatu disebalik rambut. Selepas beberapa tahun, kaedah seperti ini mula mendapat perhatian disebabkan pengwujudan pelbagai bahan multimedia terutama sekali dalam bentuk digital. Ini kerana, bahan-bahan seperti ini mempunyai kelebihan yang tertentu, iaitu :-

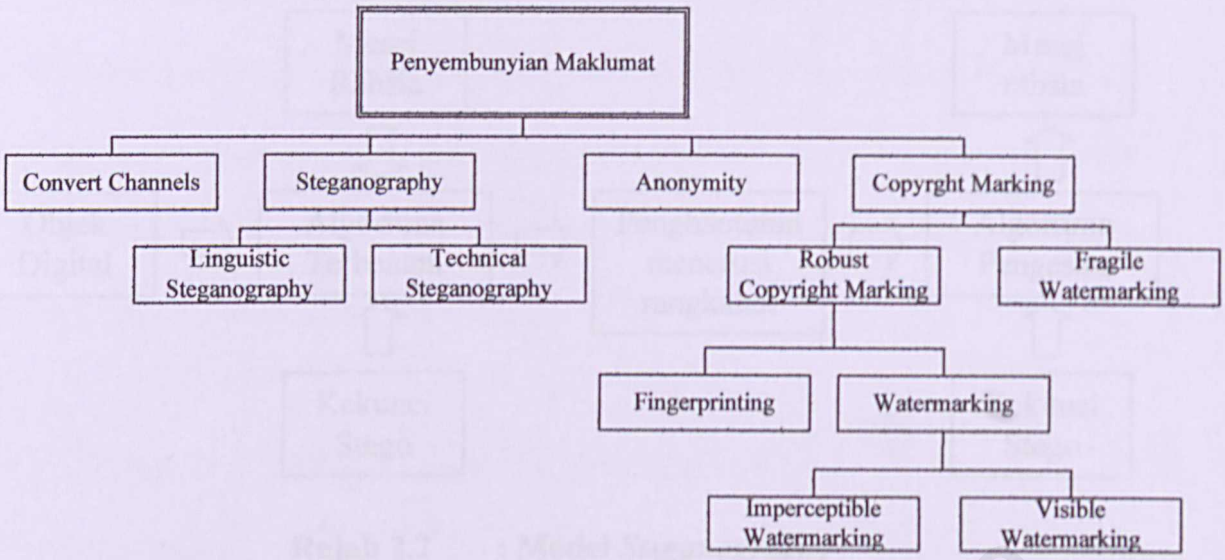
- Mudah diubahsuai dan disunting
- Tahan lama
- Lebih murah
- Senang dicapai
- Sesuai untuk diagihkan melalui rangkaian internet

Walaupun bahan-bahan digital ini mendatangkan kebaikan dalam dunia penyembunyian maklumat, terdapat juga masalah-masalah yang berlaku daripada bahan tersebut seperti :-

- Masalah pengesahan
- Masalah penyalinan dan pengagihan secara haram
- Masalah dari segi hakcipta bahan

Berikut adalah beberapa contoh dalam mengaplikasikan penggunaan kaedah penyembunyian maklumat dalam kehidupan seharian:-

1. Kementerian Pertahanan menggunakan kaedah penyembunyian maklumat untuk melindungi komunikasi antara mereka di mana isyarat komunikasi mereka akan lebih sukar untuk dikesan oleh musuh.
2. Pihak polis dan agensi-agensi tertentu menggunakan kaedah ini untuk menyembunyikan segala data dan maklumat sulit daripada dicerobohi terutama sekali ketika penghantaran dan penerimaan data tersebut oleh pegawai atasan.
3. Kerajaan Malaysia kini mengamalkan konsep mesyuarat dan pengucapan secara jarak jauh di mana konsep sedemikian perlu dilindungi agar tidak timbul masalah wujudnya orang ketiga yang tidak dikenali.

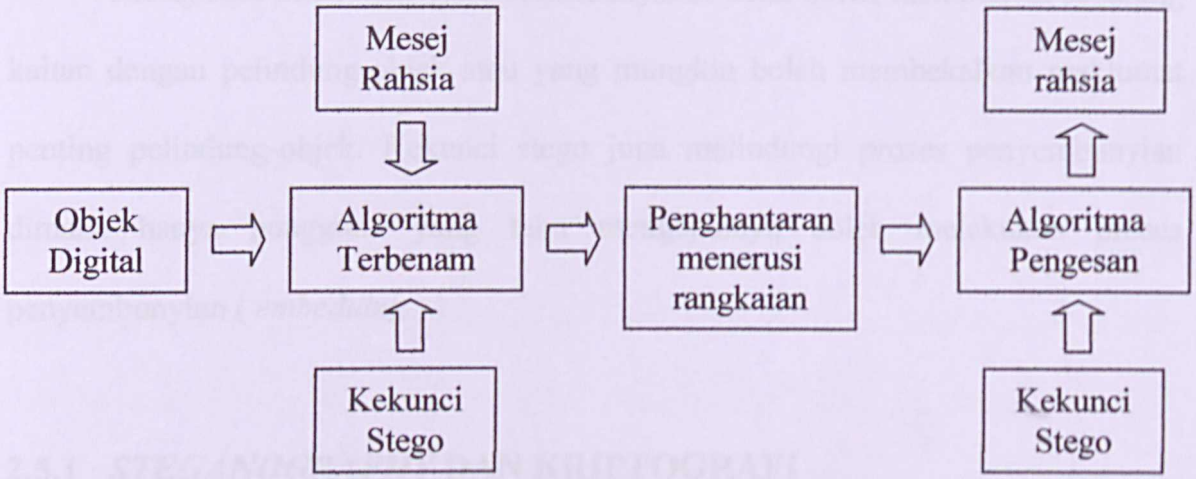


Rajah 2.1 : Kaedah-kaedah yang terdapat dalam penyembunyian maklumat.

2.5 *STEGANOGRAPHY*

Kaedah steganography adalah salah satu kaedah yang terdapat dalam penyembunyian maklumat selain kaedah *convert channels*, *anonymity* dan *copyright marking*. *Steganography* ialah seni atau sains atau kerja dalam cara berkomunikasi yang menyembunyikan satu mesej rahsia dalam maklumat utama yang lain. *Steganography* digunakan untuk menukarkan komunikasi antara dua parti atau pihak yang tidak mengetahui akan kewujudan serangan dan penceroboh lain. Tujuan utama serangan ini adalah untuk mengesan maklumat atau mesej rahsia antara dua parti atau pihak tersebut.

Model *steganography* terdiri daripada beberapa istilah yang perlu difahami dengan lebih lanjut.



Rajah 2.2 : Model *Steganography*

- Data terbenam - mesej atau maklumat yang disembunyikan dalam sesuatu yang lain yang dikenali sebagai pelindung-teks, pelindung-imej, pelindung-audio atau pelindung-objek menghasilkan objek-stego atau objek bertanda.
- Kekunci stego - kekunci yang diperlukan untuk melaksanakan proses penyembunyian dan menghalang mesej atau maklumat yang disembunyikan daripada dikenal pasti oleh pengguna-pengguna lain yang tahu akan mesej tersebut.
- Pembenaman - proses untuk menyembunyikan mesej atau maklumat di sebalik pelindung-objek.
- Pengesan - proses untuk menukarkan semula objek-stego atau pelindung-objek ke bentuk asal (*embedded data*).

Mesej atau maklumat yang disembunyikan tidak boleh mempunyai sebarang kaitan dengan pelindung-objek atau yang mungkin boleh membekalkan maklumat penting pelindung-objek. Kekunci stego juga melindungi proses penyembunyian dimana hanya pengguna yang tahu mengenainya boleh melakukan proses penyembunyian (*embedding*).

2.5.1 *STEGANOGRAPHY* DAN KRIPTOGRAFI

Steganography bermaksud melindungi data atau maklumat manakala kriptografi pula bermaksud menulis secara rahsia. Dalam penghantaran mesej atau maklumat menggunakan kaedah kriptografi, hanya penerima yang sah sahaja boleh membacanya. Mesej yang hendak dihantar dipanggil teks biasa dan mesej yang telah melalui kaedah kriptografi dipanggil teks rahsia. Proses untuk menukarkan teks biasa ke teks rahsia dikenali sebagai proses enkripsi dan proses sebaliknya dikenali sebagai dekripsi. Segala keterangan ini telah diterangkan dalam bahagian kriptografi. Walau bagaimana pun, proses enkripsi hanya melindungi kandungan mesej ketika proses penghantaran melalui rangkaian kepada penerima. Selepas penerima menerima mesej tersebut dan melakukan proses dekripsi, mesej tersebut tidak dapat dilindungi lagi. Ini berbeza dengan *steganography* yang menyembunyikan mesej di dalam objek lain tanpa melakukan sebarang perubahan pada mesej tersebut. Oleh sebab itu, *steganography* lebih luas penggunaannya dan mula diminati berbanding dengan kriptografi.

2.5.2 *STEGANOGRAPHY* DAN PENANDAAN DIGITAL

Perbezaan antara *steganography* dan penandaan digital adalah dari segi penggunaannya. Penandaan digital boleh dilihat sebagai satu pelengkap kepada pembawa dimana boleh mengandungi maklumat seperti lesen, hakcipta, pengarang dan sebagainya. *Steganography* pula tidak mengandungi maklumat-maklumat seperti yang terdapat dalam penandaan digital. Selain itu, terdapat juga masalah dari segi bandwidth untuk mesej yang disembunyikan. Tumpuan lebih diberikan kepada mesej yang menggunakan kaedah penandaan digital. Walau bagaimana pun, konsep asal *steganography* dan penandaan digital adalah sama dan kedua-dua kaedah ini menggunakan penyembunyian maklumat sebagai kaedah utama.

2.5.3 TEKNIK-TEKNIK *STEGANOGRAPHY*

Terdapat tiga keperluan utama yang diperlukan bagi setiap teknik *steganography* iaitu :-

- Mesej yang disembunyikan **tidak dapat dikesan** oleh pengguna lain.
    - Pelindung-objek yang mengandungi atau tidak mengandungi mesej disebaliknya haruslah wujud sebagai imej asal kepada semua ujian yang dilakukan terhadapnya.
    - Pengguna seharusnya mengetahui sebanyak mana maklumat mengenai sumber pelindung-objek dihasilkan.
    - Contohnya ialah sekiranya pelindung-objek diimbas menggunakan pengimbas, pelindung-objek tersebut mempunyai kaitan yang kuat

dalam arah mendatar berbanding dengan arah tegak. Ini kerana, setiap pengimbas mempunyai maklumat terperinci tentang hingar dan perlu diberi perhatian sekiranya mendatangkan masalah, teknik steganography yang mempunyai ciri-ciri keselamatan yang kuat diperlukan.

- Pelindung-objek yang digunakan mestilah tidak dapat dibezakan daripada imej yang asal.

- **Kapasiti** saluran komunikasi.
  - Sekiranya satu imej boleh menyembunyikan satu bit maklumat ke dalam satu rangka pelindung-objek tanpa mengambil kira hingar, saluran komunikasi mungkin akan kekurangan jalur lebar.
  - Masalahnya ialah untuk menyembunyikan seberapa banyak maklumat yang mungkin sambil dapat sesuaikan dengan imej yang mempunyai hingar.
- Mesej yang tersembunyi **boleh dikesan** tanpa imej yang asal.

Terdapat tiga kaedah utama untuk menyembunyikan data, mesej atau maklumat, iaitu :-

1. Penyembunyian disebalik teks.
2. Penyembunyian disebalik imej (bergantung kepada format imej).
3. Penyembunyian disebalik audio (bergantung kepada format audio).

Terdapat beberapa teknik utama steganography yang digunakan, iaitu :-

1. Teknik *Analog of One-time pad.*
2. Teknik *LSB encoding.*
3. Teknik *Spread Spectrum Systems.*
4. Teknik Penyembunyian Gema.
5. Teknik Pengekodan Anjakan-Baris.
6. Teknik Pengekodan Anjakan-Huruf.
7. Teknik *Feature Specific Coding.*
8. Teknik Semantik.
9. Teknik Sintaks.
10. Teknik *Low-bit Encoding.*
11. Teknik Pengekodan fasa.

Teknik-teknik ini akan diaplikasikan bergantung kepada kaedah untuk menyembunyikan maklumat yang digunakan. Setiap kaedah mempunyai teknik-teknik tertentu.

2.5.4 PENYEMBUNYIAN DISEBALIK TEKS

Teks boleh digunakan sebagai satu kaedah menyembunyikan mesej rahsia menggunakan *steganography*. Ini boleh disempurnakan dengan melakukan anjakan teks yang asal ke kiri atau kanan, atas atau bawah serta menukarkan panjang teks-teks tertentu secara mendatar atau menegak. Kesemua teknik menggunakan teks memerlukan kefahaman mengenai teks yang asal supaya dapat menghasilkan semula mesej rahsia selepas disembunyikan. Hanya jumlah data yang kecil sahaja boleh

disembunyikan melalui cara ini. Oleh sebab itu, cara ini mempunyai kadar data yang rendah berbanding dengan cara-cara lain. Teknik-teknik *steganography* yang digunakan dalam cara ini ialah :-

- Pengekodan Anjakan-Baris
- Pengekodan Anjakan-Huruf
- *Feature Specific Coding*
- Semantik
- Sintaks

2.5.4.1 TEKNIK PENGEKODAN ANJAKAN-BARIS

Teknik pengekodan anjakan-baris melakukan anjakan 1/300 barisan teks setiap satu inci menaik dan menurun secara menegak. Teknik ini muncul sebagai teknik paling nyata kepada pengguna. Selain itu, teknik ini adalah teknik yang paling susah untuk mengesan mesej rahsia, disebabkan mengubah data akan menyebabkan mesej rahsia yang tersembunyi akan musnah.

2.5.4.2 TEKNIK PENGEKODAN ANJAKAN-HURUF

Teknik pengekodan anjakan-huruf pula mempuyai persamaan dengan teknik pengekodan anjakan-baris. Lokasi mendatar teks akan dianjak ke kiri atau ke kanan mengikut barisan teks. Teknik ini mempunyai kebolehan mengesan sama seperti teknik pengekodan anjakan-baris Cuma perbezaannya ialah kebolehan mengesannya lebih kurang berbanding pengekodan anjakan-baris. Namun demikian, jarak atau

ruang teks antara satu sama lain hendaklah dikekalkan supaya teknik ini dapat disempurnakan seperti teks pewajaran.

2.5.4.3 TEKNIK *FEATURE SPECIFIC CODING*

Teknik *feature specific coding* mengekod satu mesej rahsia kepada satu bentuk teks yang diformatkan dengan melakukan pengubahsuaian kepada saiz pada beberapa huruf tertentu dalam format mendatar dan menegak. Setiap bit boleh ditukarkan ke bentuk teks dengan mengubahsuai saiz huruf-huruf seperti a,b,c dan sebagainya. Teknik ini disempurnakan dengan memanjangkan atau memendekkan baris-baris menegak yang tinggi pada huruf-huruf tersebut.

2.5.4.4 TEKNIK SEMANTIK

Teknik semantik memanipulasikan setiap perkataan dengan menggantikannya dengan sinonim perkataan tersebut. Teknik ini mempunyai masalah apabila setiap perkataan tidak dapat ditukar kepada sinonim yang betul terutama sekali mesej atau maklumat yang menggunakan bahasa Inggeris. Contohnya perkataan *sick* dan *ill* mempunyai sinonim yang sama. Kedua-duanya boleh wujud sebagai kata sifat cuma kadang-kala perkataan *sick* boleh digunakan sebagai kata nama. Perkataan *ill* mempunyai maksud yang berlainan yang tidak sama dengan perkataan *sick*.

2.5.4.5 TEKNIK SINTAKS

Teknik sintaks menggunakan cara meletakkan tanda bacaan. Kesalahan dalam tanda bacaan boleh dilihat dengan mudah dan perubahan dalam susunan ayat pada mesej boleh mengubah maksud asal ayat tersebut.

2.5.5 PENYEMBUNYIAN DISEBALIK AUDIO

Penyembunyian disebalik audio diadaptasi daripada bagaimana sistem pengauditan manusia (HAS) mentafsirkan bunyi. Cara ini menjadi semakin mencabar sejak HAS menjadi semakin sensitif. HAS mengecilkan bunyi yang besar dan menenggelamkan bunyi yang perlahan. Kedua-dua kelemahan ini dapat diatasi dengan wujudnya cara penyembunyian disebalik audio. Teknik-teknik yang digunakan dalam cara ini ialah :-

- *Low-bit Encoding*
- Pengekodan Fasa
- Perebakan spektrum
- Penyembunyian Gema

2.5.5.1 TEKNIK *LOW-BIT ENCODING*

Teknik *low-bit encoding* mengekod satu rentetan binari dalam least significant bit (LSB) sesuatu fail audio. Walaupun jumlah data yang boleh ditukarkan dalam isyarat audio adalah besar, teknik ini dengan mudah boleh

dimusnahkan oleh hingar saluran. Data-data lebih mudah dimusnahkan sewaktu penghantaran lain berbanding penghantaran digital ke digital.

2.5.5.2 TEKNIK PENGEKODAN FASA

Teknik pengekodan fasa menggantikan fasa dalam setiap segmen audio dengan fasa rujukan yang mewakili setiap data. Teknik ini adalah berdasarkan pada kepekaan HAS untuk pelbagai fasa. Setiap fail bunyi dibahagikan kepada blok-blok dan setiap blok menandakan fasa telah diubahsuai untuk menyembunyikan maklumat.

2.5.5.3 TEKNIK PEREBAKAN SPEKTRUM

Teknik perebakan spektrum menukarkan aliran maklumat dengan memanjangkan atau melebarkan data mengikut seberapa banyak spektrum frekuensi. Ini membenarkan penerimaan isyarat, walaupun jika terdapat gangguan pada beberapa frekuensi. Ini juga biasanya akan menambahkan hingar kepada audio tersebut. Menyembunyikan isyarat-isyarat boleh disaring supaya komponen-komponen yang terdapat bunyi-bunyi tambahan dapat dikurangkan kuasanya.

2.5.5.4 TEKNIK PENYEMBUNYIAN GEMA

Teknik penyembunyian gema menyembunyikan data ke dalam isyarat audio dengan memperkenalkan kaedah gema. Tiga perbezaan pada gema iaitu dari segi amplitud, kadar penangguhan dan kadar pengimbangan, setiap data dapat

disembunyikan. Kadar pendengaran manusia tidak dapat membezakan antara dua isyarat disebabkan kadar pengimbangan antara audio yang asal dan penurunan gema dan kedua-dua isyarat digabungkan sekali. Teknik ini mempunyai kadar kejayaan yang tinggi.

2.5.6 PENYEMBUNYIAN DISEBALIK IMEJ

Imej ialah tatasusunan nombor yang mewakili piksel-piksel. Imej digital disimpan di dalam 24-bit atau 8-bit setiap piksel. Piksel-piksel ini memberi banyak kelebihan di mana maklumat boleh ditukarkan ke satu bentuk imej. Teknik-teknik yang digunakan untuk cara ini ialah :-

- *Least Significant Bit* (LSB)
- Penyamaran dan Penyaringan (Masking and Filtering)
- Algoritma dan Penjelmaan (Algorithms and transformations)

2.5.6.1 TEKNIK *LEAST SIGNIFICANT BIT* (LSB)

Teknik *least significant bit* (LSB) ialah teknik yang paling kerap digunakan disebabkan paling mudah untuk disempurnakan. Data akan diselitkan ke dalam bahagian yang sedikit dan kedua bit yang sedikit bagi piksel. Teknik ini boleh dikesan kerana terdapat perubahan pada piksel-piksel di mana akan menyebabkan perubahan pada warna. Pemilihan sebagai pelindung-objek hendaklah diberi perhatian supaya segala perubahan pada warna tidak dapat diketahui. Penggunaan imej atau gambar yang kerap digunakan seharusnya tidak menggunakan teknik ini untuk menyembunyikan maklumat atau mesej.

2.5.6.2 TEKNIK PENYAMARAN DAN PENYARINGAN

Teknik penyamaran dan penjelmaan (*masking and filtering*) menyerupai teknik penandaan digital (satu corak bit-bit dimuatkan ke dalam satu fail imej yang mengenal pasti maklumat hakcipta fail, pengarang dan sebagainya). Kegunaan penandaan digital wujud daripada kaedah penandaan. Penandaan berbeza dengan *steganography* walaupun konsep yang digunakan adalah sama. Ini kerana, *steganography* menyembunyikan dan melindungi setiap data dalam imej manakala penandaan pula ialah bit-bit asal dipecahkan dan diselerakkan keseluruh imej supaya teknik ini tidak boleh dimanipulasikan dan dikenalpasti.

2.5.6.3 TEKNIK ALGORITMA DAN PENJELMAAN

Teknik algoritma dan penjelmaan (*algorithms and transformation*) digunakan untuk menghantar imej berformat JPEG melalui internet. Satu contoh penjelmaan ialah spread-spectrum. Komunikasi spread-spectrum menghantar satu isyarat jalur sempit menerusi satu lebar jalur yang lebih besar supaya kepadatan spektrum dalam saluran dilihat seperti hingar. Selain itu, teknik ini boleh mengubah *luminance*, menyembunyikan maklumat dengan membahagikan lebar jalur kepada beberapa saluran dan mengubahsuai kecerahan blok-blok piksel.

2.5.7 PENYEMBUNYIAN DATA

Sasaran utama *steganography* ialah untuk menyembunyikan dan melindungi data. Terdapat beberapa ciri dan batasan yang perlu dititikberatkan untuk menyembunyikan data dengan jayanya. Sasaran utama data pula ialah terus kekal tersembunyi disebalik pelindun-objek. Terdapat beberapa panduan yang mewakili ciri-ciri dan batasan-batasan apabila menyembunyikan data, iaitu :-

- Setiap pelindung-objek yang digunakan hendaklah dikekalkan keasliannya ketika penyembunyian data dilakukan. Sehubungan itu, pelindung-objek tidak boleh ada apa-apa perubahan terutama sekali pada komposisi warna. Biasanya saiz pelindung-objek akan menjadi lebih besar berbanding yang asal dan ini menimbulkan keraguan kepada pengguna-pengguna lain.
- Penyembunyian data hendaklah dilakukan secara terus ke dalam pelindung-objek. Penyembunyian data perlu dilakukan dengan sempurna menerusi format fail yang berbeza.
- Penyembunyian data hendaklah kebal daripada segala manipulasi. Ini termasuklah pengubahsuaian secara sengaja atau pengubahsuaian ketika penghantaran.
- Kesalahan membetulkan kod-kod hendaklah dimuatkan terus ke dalam pelindung-objek untuk memastikan keaslian data apabila pelindung-objek diubahsuai.

2.6 SERANGAN

Percubaan untuk mengesan kewujudan data *steganography* dikenali sebagai serangan. Biasanya serangan terbahagi kepada dua iaitu serangan secara aktif dan serangan secara pasif. Serangan secara aktif, penceroboh boleh menyekat data, mesej atau maklumat yang tersembunyi. Bagi serangan secara pasif pula, penceroboh boleh memanipulasi data, mesej atau maklumat yang tersembunyi. Pengguna yang menggunakan kaedah *steganography* haruslah berhati-berhati apabila memilih teknik yang sesuai bagi mengelakkan serangan secara aktif atau pasif. Teknik yang digunakan hendaklah lebih effektif, dipercayai dan boleh melawan serangan dengan kuat. Terdapat empat jenis kumpulan serangan, iaitu :-

- Serangan keteguhan
  - Kategori ini termasuklah serangan untuk menghilangkan mesej atau data yang disembunyikan tanpa mengurangkan kualiti produk yang terlibat.
- Serangan persembahan
  - Kategori ini membuang mesej atau maklumat yang disembunyikan. Serangan ini memanipulasi kandungan yang disembunyikan di mana serangan ini tidak dapat dikesan.
- Serangan tafsiran
  - Bagi kategori ini pula, penyerang bertujuan untuk mencipta satu situasi baru di mana situasi ini menghalang tuntutan pemilik dan menjadikan penyembunyian data tidak boleh dipercayai lagi.

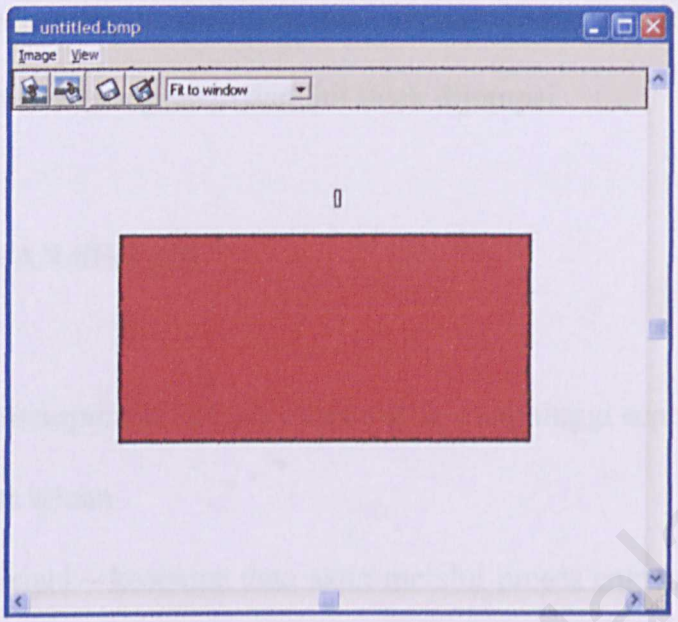
- Serangan rasmi
  - Kategori ini berlainan dengan kategori-kategori yang lain disebabkan kategori ini melibatkan kesemua perbuatan yang boleh diambil tindakan mahkamah kerana menghapuskan kredibiliti penandaan sebagai bukti pemilik hakcipta. Serangan ini tidak melibatkan memanipulasi produk yang terlibat tetapi serangan ke atas pemilik dan mencabar kredibiliti pemilik.

2.7 SISTEM YANG SEDIA ADA

Terdapat beberapa sistem *steganography* yang telah dibangunkan. Sistem-sistem ini bertindak menjadi panduan kepada sistem *steganography* yang akan dibangunkan. Antara sistem-sistem steganography tersebut ialah :-

- Sistem HIP 2.0
- Sistem S-Tools
- Sistem Courier

2.7.1 SISTEM HIP 2.0



Rajah 2.3 : Antaramuka Sistem HIP 2.0

2.7.1.1 LATAR BELAKANG SISTEM

Sistem HIP (*Hide In Picture*) adalah sistem yang digunakan untuk menyembunyikan data dalam sesuatu imej berformat bitmap dengan melakukan pengubahsuaian pada komposisi warnanya yang tidak dapat dikesan dengan penglihatan manusia. Apabila sesuatu fail disembunyikan, imej yang digunakan sebagai pelindung-objek akan menyembunyikan setiap bahagian fail di dalam kawasan imej tersebut. Kawasan yang digunakan untuk menyimpan setiap bahagian fail tersebut ditentukan dengan melakukan beberapa pengiraan bersama-sama kata laluan yang digunakan. Apabila hendak mendapatkan semula fail yang disembunyikan, pengiraan yang sama dilakukan pada kata laluan dan mengetahui

kawasan yang mana mengandungi setiap bahagian fail tersebut supaya fail yang disembunyikan dapat dibentuk semula. Jika kata laluan yang digunakan adalah tidak betul semasa mendapatkan semula fail yang disembunyikan, sistem HIP akan cuba membaca pada kawasan yang salah dan fail tidak dijumpai.

2.7.1.2 KELEBIHAN SISTEM

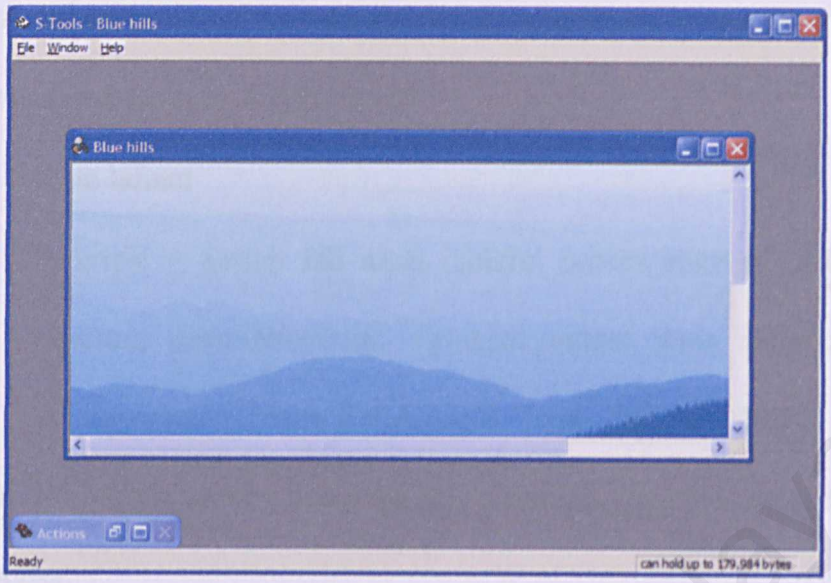
1. Sistem ini mempunyai ciri-ciri keselamatan yang tinggi seperti :-
    - Kata laluan
    - Enkripsi – kesemua data akan melalui proses enkripsi terlebih dahulu sebelum disembunyikan ke dalam imej. Ini penting untuk meningkat keselamatan daripada pencerobohan. Sistem HIP menawarkan dua jenis algoritma enkripsi iaitu *Blowfish* dan *Rijndael*. Pengguna boleh memilih algoritma enkripsi yang bersesuaian .
2. Sistem ini mempunyai ciri pemadaman fail.
    - Ciri pemadaman fail digunakan untuk mengalihkan fail yang disembunyikan terlebih dahulu. Jika pengguna menggunakan kata laluan yang betul ketika pemadaman fail dilakukan, hanya kawasan yang diperlukan sahaja akan ditindih dengan fail yang baru dan menyebabkan kehilangan kualiti imej tidak terjejas. Jika kata laluan yang digunakan tidak betul, fail tidak dapat dipadam dengan bersih dan fail akan disimpan di pelbagai kawasan dan menyebabkan kehilangan kualiti imej adalah ketara.

3. Sistem ini juga turut mempunyai ciri menjadikan warna-warna tertentu imej lutsinar.
    - Warna pada imej boleh dijadikan lutsinar dan di kawasan ini tidak boleh digunakan sebagai tempat menyembunyikan fail. Ini penting apabila penyembunyian fail di lakukan menggunakan imej daripada laman web.
4. Pengguna boleh menamakan dengan nama lain untuk fail yang disembunyikan.

2.7.1.3 KEKURANGAN SISTEM

1. Sistem ini membenarkan hanya fail sahaja boleh disembunyikan.
2. Hanya imej berformat bitmap sahaja dibenarkan untuk bertindak sebagai pelindung-objek.

2.7.2 SISTEM S-TOOLS



Rajah 2.4 : Antaramuka Sistem S-tools

2.7.2.1 LATAR BELAKANG SISTEM

Sistem S-tools ialah salah satu sistem *steganography* yang digunakan untuk menyembunyikan fail di dalam imej yang berformat BMP dan GIF serta di dalam bunyi yang berformat WAV. Setiap fail yang hendak disembunyikan akan dimampatkan sebelum melalui proses enkripsi dan disembunyikan. Sistem ini membenarkan beberapa fail disembunyikan secara serentak. Selain itu, sistem ini menggunakan teknik *Least Significant Bit* (LSB) untuk bunyi dan teknik Perebakan Spektrum untuk gambar.

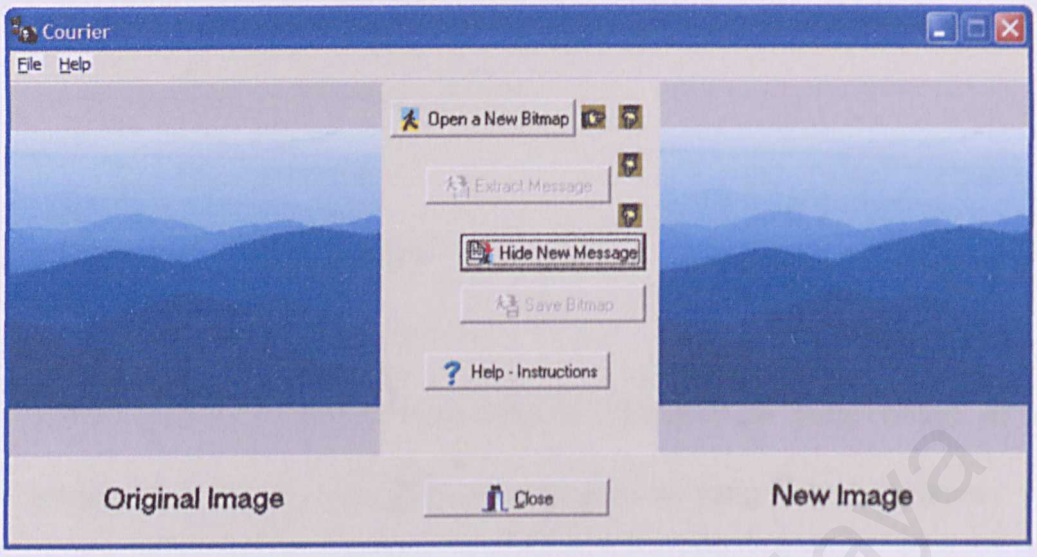
2.7.2.2 KELEBIHAN SISTEM

1. Sistem ini mempunyai persamaan dengan sistem HIP yang mempunyai ciri-ciri keselamatan yang tinggi seperti :-
    - Kata laluan
    - Enkripsi – Setiap fail akan melalui proses enkripsi terlebih dahulu sebelum disembunyikan. Terdapat empat jenis algoritma enkripsi dalam sistem ini iaitu IDEA, DES, Triple DES dan MDC.
2. Sistem ini membenarkan beberapa fail disembunyikan secara serentak dalam satu masa.
3. Sistem ini juga membenarkan fail disembunyikan samada melalui imej atau bunyi yang bertindak sebagai pelindung-objek.
4. Sistem ini mempunyai ciri pemadatan di mana setiap fail akan dipadatkan terlebih dahulu sebelum disembunyikan.
5. Pengguna boleh menamakan dengan nama lain untuk fail yang disembunyikan.

2.7.2.3 KEKURANGAN SISTEM

1. Sistem ini membenarkan data yang berbentuk fail sahaja untuk disembunyikan.
2. Hanya imej berformat BMP dan GIF serta bunyi yang berformat WAV sahaja boleh digunakan sebagai pelindung-objek.
3. Sistem ini tidak sesuai dengan versi-versi yang terlebih dahulu dibangunkan.

2.7.3 SISTEM COURIER



Rajah 2.5 : Antaramuka Sistem Courier

2.7.3.1 LATAR BELAKANG SISTEM

Sistem Courier adalah sistem yang digunakan untuk penyembunyian mesej mudah yang membenarkan mesej teks disembunyikan disebalik imej bitmap. Kewujudan mesej tidak dapat dikesan oleh pengguna-pengguna lain yang melihat imej bitmap tersebut. Hanya pengguna yang mempunyai sistem yang sama boleh membaca mesej disebalik imej bitmap tersebut.

2.7.3.2 KELEBIHAN SISTEM

1. Sistem ini membenarkan pengguna menyembunyikan mesej sehingga 357300 huruf disebalik imej bitmap tersebut.

2.7.3.3 KEKURANGAN SISTEM

1. Sistem ini tidak mempunyai ciri-ciri keselamatan yang tinggi di mana pengguna-pengguna lain boleh membaca mesej yang disembunyikan.
2. Hanya imej berformat BMP sahaja boleh digunakan sebagai pelindung-objek.
3. Hanya mesej teks sahaja dibenarkan untuk disembunyikan.

2.8 PERBANDINGAN SISTEM

Daripada pemerhatian pada sistem-sistem yang sedia ada, terdapat beberapa kelebihan yang akan turut diaplikasikan pada sistem *steganography* yang akan dibangunkan. Kelebihan seperti penggunaan kata laluan untuk membaca teks atau fail yang tersembunyi memberi tahap keselamatan yang tinggi pada data yang disembunyikan. Namun demikian, kebanyakan sistem yang sedia ada hanya menggunakan satu jenis data sahaja untuk disembunyikan samada menggunakan fail atau maklumat berbentuk teks. Untuk mengaplikasikan kedua-duanya dalam satu sistem yang sama, sistem *steganography* dibangunkan untuk mengatasi masalah dan kekurangan yang terdapat pada sistem-sistem tersebut. Walau bagaimana pun, sistem *steganography* yang dibangunkan tetap akan menggunakan imej yang berformat bitmap sahaja. Ini kerana, imej-imej yang berformat lain kadang-kala menimbulkan

masalah sebagai pelindung-objek yang selamat. Oleh sebab itu, sistem *steganography* yang akan dibangunkan tetap menggunakan imej yang berformat bitmap sahaja.

BAB 3
METODOLOGI

BAB 3

METODOLOGI

3.1 METODOLOGI SISTEM

Metodologi sistem terdiri daripada beberapa proses tertentu yang melibatkan aktiviti dan sumber sebelum dapat menghasilkan keputusan atau output yang dikehendaki. Metodologi ini menunjukkan turutan perjalanan bagi setiap proses atau aktiviti dalam pembangunan sistem. Secara amnya, kitaran pembangunan sistem mengandungi beberapa fasa utama, iaitu :-

- Fasa analisis keperluan dan spesifikasi
- Fasa rekabentuk
    - rekabentuk permulaan
    - rekabentuk terperinci
- Fasa perlaksanaan
- Fasa pengujian
    - pengujian unit
    - pengujian sistem
    - pengujian penyepaduan atau integrasi
- Fasa penyelenggaraan

Metodologi ialah satu susunan model pembangunan sistem yang disertakan bersama-sama dengan satu atau lebih teknik pembangunan sistem. Selain itu, metodologi juga adalah satu piawaian yang telah diperakui dan disahkan agar dituruti

oleh individu-individu yang terlibat dalam pembangunan sistem. Pemilihan metodologi yang baik dan bersesuaian dengan sistem akan menghasilkan satu sistem yang lebih baik dan dipercayai. Sebelum membangunkan sesuatu sistem, setiap metodologi haruslah diteliti dengan baik supaya menepati ciri-ciri domain masalah yang sebenar.

Terdapat beberapa objektif dalam penggunaan metodologi yang dipilih dan digunakan, iaitu :-

1. Perisian atau sistem yang dibangunkan dapat berjalan dengan lancar tanpa menghadapi sebarang rintangan atau halangan yang mungkin wujud. Sehubungan itu, perancangan masa dan anggaran kos yang telah dirancang pada permulaan projek dapat ditepati sekaligus menghasilkan satu perisian yang berkualiti tinggi.
2. Untuk memberitahu individu-individu yang terlibat dalam pembangunan projek supaya sedia maklum akan aktiviti yang terlibat, sumber yang digunakan dan rintangan yang akan wujud.
3. Untuk membantu mengenalpasti ketidakseimbangan dan kelimpahan sistem yang mungkin wujud melalui pemerhatian pada keseluruhan proses.
4. Untuk memahami tahap pengabstrakan, kawalan aliran dan penjujukan sesuatu sistem yang dibangunkan dengan lebih mendalam.
5. Untuk membahagikan setiap sistem kepada langkah-langkah atau fasa yang bersesuaian untuk disempurnakan mengikut syarat.

Selain daripada objektif metodologi sistem, terdapat juga faedah-faedah yang boleh didapati dalam menggunakan metodologi yang bersesuaian. Antaranya ialah :-

1. **Dapat meningkatkan produktiviti sesuatu sistem yang dibangunkan.**

   Ini kerana, setiap perisian yang menggunakan metodologi yang bersesuaian dapat menghindarkan segala masalah-masalah dan kehendak pengguna dapat dipenuhi.

2. **Dapat mengurangkan kos dalam pembangunan sistem.**

   Ini disebakan setiap masalah dapat dikesan dengan lebih awal dan mengambil masa yang lebih singkat untuk membaikinya. Oleh sebab itu, kos yang digunakan juga adalah rendah berbanding kos asal yang telah ditetapkan.

3. **Dapat menghasilkan satu dokumentasi yang lebih baik.**

   Setiap aktiviti, proses dan kaedah pembangunan didokumenkan dengan baik, terang dan jelas untuk dijadikan sebagai panduan.

4. **Jangka hayat penyelenggaraan dapat dikurangkan.**

   Setiap masalah dapat dikesan pada peringkat awal dan ini dapat memberikan kelebihan kepada pembangun dan ahli-ahli projek yang lain untuk menyelenggara setiap masalah mengikut peringkat demi peringkat dengan lebih cepat tanpa menunggu sehingga projek tersebut selesai.

5. **Dapat menjimatkan masa dalam pembangunan sistem.**

   Penjimatan masa dapat dipenuhi kerana setiap aktiviti yang dilakukan adalah berdasarkan fasa-fasa yang telah dibahagikan dan ditetapkan. Setiap ahli projek akan melakukan kerja-kerja mengikut fasa yang telah ditetapkan dan ini akan menjadikan perancangan masa dapat dituruti dengan lebih mudah.

3.2 JENIS-JENIS METODOLOGI

Terdapat pelbagai metodologi boleh digunakan dalam setiap pembangunan sistem. Setiap metodologi yang digunakan mempunyai kelebihan dan kelemahan yang tersendiri. Kelebihan dan kelemahan ini dijadikan sebagai panduan dan rujukan setiap pembangun sistem untuk menilai metodologi yang harus dipilih dalam pembangunan sistem mereka. Pembangun sistem lebih gemar menggunakan metodologi yang lebih mudah difahami dan diikuti untuk dilaksanakan dalam pembangunan sistem mereka. Antara metodologi-metodologi yang sering menjadi pilian pembangun sistem ialah :-

- Model Air Terjun (*Waterfall*)
- Model V
- Model Air Terjun bersama Pemprototaipan
- Model Berlingkar (*Spiral*)
- Model Prototaip

3.3 METODOLOGI YANG DIPILIH

Metodologi yang dipilih untuk digunakan dalam pembangunan sistem *steganography* ialah model Air Terjun bersama Prototaip. Model Air Terjun bersama Protaip ini dipilih disebabkan struktur modelnya menunjukkan setiap proses secara tersusun dalam pembangunan sistem dari awal sehinggalah terbentuknya sistem *steganography*. Selain itu, proses-proses dalam setiap fasa model ini akan diselesaikan dahulu sebelum melangkah ke fasa berikutnya. Ini kerana, setiap fasa dalam model ini dilengkapi dengan batu tanda (*milestone*). Batu tanda ini ditakrifkan sebagai satu set dokumen yang telah lengkap dan apabila dokumen dipersetujui oleh setiap ahli dan pembangun sistem, fasa berikutnya akan dilakukan. Disamping itu juga, model Air Terjun bersama Prototaip adalah model yang melibatkan jujukan literasi dan mempunyai hubung kait dalam setiap proses-proses pembangunan sistem.

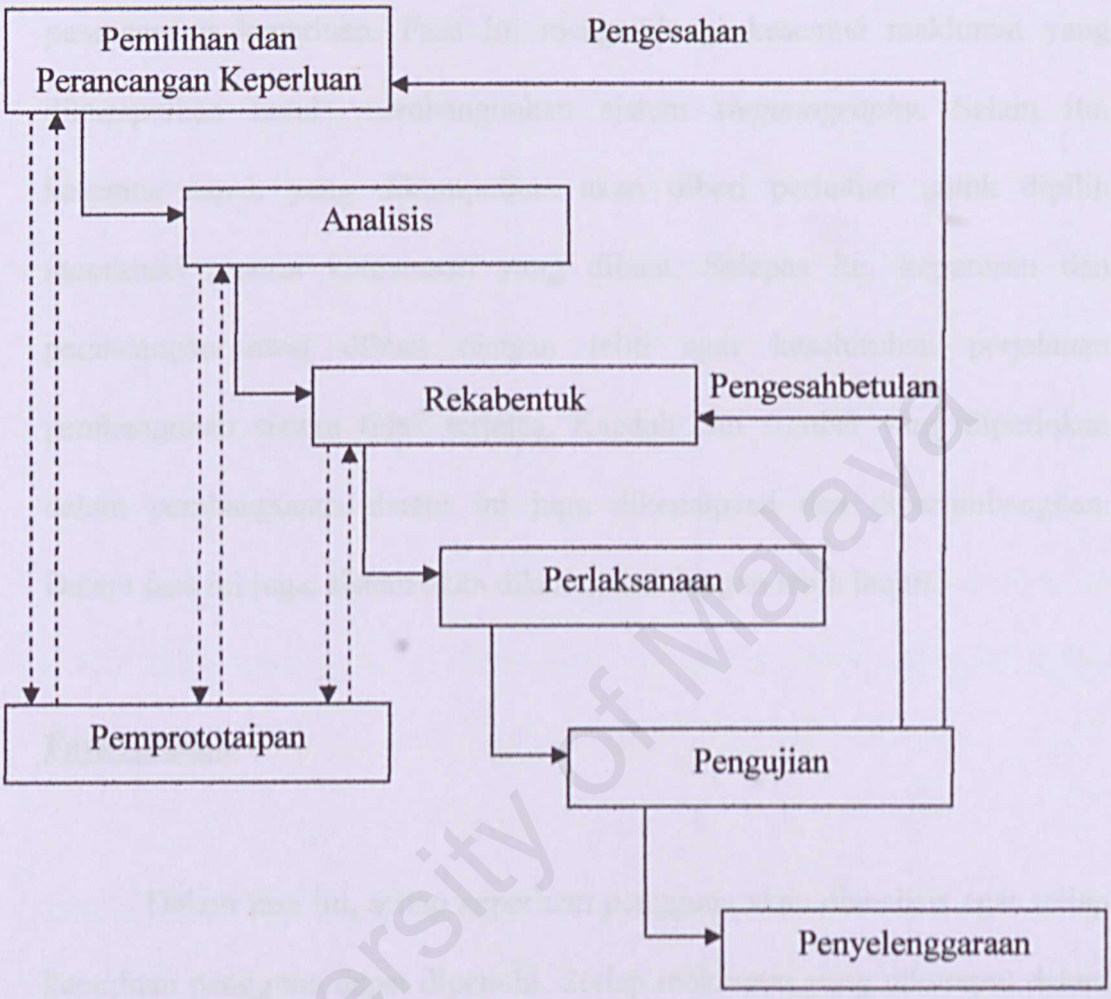
3.3.1 KELEBIHAN MODEL AIR TERJUN (*WATERFALL*) BERSAMA PROTOTAIP

Terdapat beberapa kelebihan pada model ini berbanding dengan model-model yang lain, iaitu :-

1. Dapat mengesan masalah di peringkat awal kerana setiap fasa akan diselesaikan terlebih dahulu sebelum melangkah ke fasa berikutnya. Masalah-masalah besar akan dapat dikurangkan kerana setiap masalah kecil dapat di atasi dengan segera. Sehubungan itu, penggunaan masa dapat dijimatkan dan penggunaan kos dapat dikurangkan. Ini akan menjadikan sistem lebih berkualiti tinggi.

2. Model ini sangat terkenal dikalangan para pembangun sistem yang lain. Ini kerana, struktur model ini lebih senang difahami dan dilaksanakan berbanding dengan model-model lain. Perlaksanaan yang mudah ini akan menjadikan setiap keperluan dalam sistem dapat dipenuhi.
3. Dapat membantu mengawal setiap proses dengan menambahkan proses-proses kecil untuk meningkatkan lagi pemahaman mengenai apa yang berlaku dalam sesuatu sistem yang akan dibangunkan.
4. Pengguna akan lebih senang memahami keadaan sistem yang sebenarnya kerana model ini membenarkan interaksi antara pengguna, pembangun sistem dan sistem itu sendiri seperti apa yang diperlukan oleh sistem dan bagaimana sistem berfungsi.
5. Pembangun sistem akan lebih mendapat maklum balas daripada pengguna mengenai masalah yang dihadapi oleh pengguna ketika menggunakan sistem tersebut. Ini dapat menjadikan interaksi antara pengguna dan sistem lebih baik serta memahami fungsi-fungsi yang sukar digunakan oleh pengguna.
6. Paradigma yang digunakan dalam model ini adalah biasa, mudah dan mempunyai banyak fasa yang saling berkaitan antara satu sama lain.
7. Terdapat aktiviti pengesahan dan pengesahbetulan pada fasa pengujian. Aktiviti pengesahan dilakukan untuk memeriksa samada sistem yang dibangunkan memenuhi kehendak pengguna atau sebaliknya. Aktiviti pengesahbetulan pula dilakukan untuk memeriksa sistem yang dibangunkan adalah betul dari segi pengekodan, perisian yang digunakan dan sebagainya.

3.3.2 MODEL AIR TERJUN (*WATERFALL*) BERSAMA PROTOTAIP



Rajah 3.1 : Model Air Terjun Bersama Prototaip

Model ini terdiri daripada enam fasa utama iaitu fasa pemilihan dan perancangan keperluan, fasa analisis, fasa rekabentuk, fasa perlaksanaan, fasa pengujian dan juga fasa penyelenggaraan. Setiap fasa mengandungi proses-proses tertentu untuk dilaksanakan. Huraian mengenai setiap fasa adalah seperti berikut :-

Fasa Pemilihan dan Perancangan Keperluan

Fasa pertama yang terdapat dalam model ini ialah pemilihan dan perancangan keperluan. Fasa ini mengandungi kesemua maklumat yang dikumpulkan untuk membangunkan sistem *steganography*. Selain itu, kesemua aspek yang dikumpulkan akan diberi perhatian untuk dipilih memasuki senarai keutamaan yang dibuat. Selepas itu, keputusan dan perancangan awal dibuat dengan teliti agar keseluruhan perjalanan pembangunan sistem tidak terjejas. Kaedah dan sumber yang diperlukan dalam pembangunan sistem ini juga dikenalpasti dan dipertimbangkan. Dalam fasa ini juga, sistem akan dikenalpasti dengan lebih lanjut.

Fasa Analisis

Dalam fasa ini, setiap keperluan pengguna akan dianalisis agar setiap keperluan pengguna dapat dipenuhi. Setiap maklumat yang dikumpul dalam fasa pertama juga akan dianalisis dengan lebih lanjut dari pelbagai aspek. Bahan-bahan yang dianalisis untuk pembangunan sistem ini termasuklah maklumat bercetak seperti artikel, buku dan majalah, sistem-sistem yang sedia ada, keterangan daripada penyelia dan sebagainya. Setiap kelemahan dan kelebihan akan dipertimbangkan mengikut kesesuaian sistem yang akan dibangunkan. Disamping itu juga, setiap fungsi dan halangan akan dikenalpasti. Fasa analisis ini adalah gambaran kepada pelan pengurusan projek.

Fasa Rekabentuk

Dalam fasa ini pula, setiap keperluan dan bukan keperluan fungsi sistem ditentukan. Selain itu, senibina keseluruhan sistem ditentukan mengikut kesesuaian sistem. Fasa rekabentuk dibahagikan kepada dua bahagian utama iaitu rekabentuk permulaan dan rekabentuk secara terperinci. Rekabentuk permulaan melibatkan rekabentuk secara am dan setiap rekabentuk sistem yang sedia ada dipertimbangkan dan dianalisa mengikut keperluan sistem *steganography*. Rekabentuk secara terperinci pula melibatkan rekabentuk sistem menggunakan perisian dan teknologi yang sedia ada. Antaramuka pentadbir, pengguna dan struktur direkabentuk untuk sistem. Disamping itu juga, carta aliran data dilukis untuk menggabungkan setiap fungsi sistem.

Fasa Perlaksanaan

Fasa perlaksanaan mengandungi beberapa proses iaitu :-

- Pengekodan
- Pemasangan
- Pengujian

Setiap proses-proses di atas dilakukan secara berperingkat ke atas sistem yang dibangunkan. Pengekodan dilakukan berdasarkan bahasa pengaturcaraan yang dipilih pada fasa pertama dan kedua. Pemasangan pula melibatkan proses gabungan pengekodan ke atas sistem menerusi perisian

yang sesuai. Perlaksanaan ini perlu dilakukan dengan teliti agar setiap fungsi dapat dijalankan mengikut yang dikehendaki pada awalan fasa.

Fasa Pengujian

Sistem yang telah lengkap dibangunkan akan diuji tahap keberkesanannya. Fasa pengujian ini penting untuk mengesan ralat dan masalah yang terdapat di dalam sistem, menentukan samada keperluan pengguna dipenuhi atau tidak dan kesannya pada masa akan datang. Terdapat tiga pengujian utama yang dilakukan ke atas sistem, iaitu :-

- Pengujian unit
  - setiap unit sistem diuji secara berperingkat.
- Pengujian sistem
  - sistem yang telah siap dibangunkan akan diuji untuk memastikan sistem dapat dijalankan tanpa sebarang masalah.
- Pengujian penyepaduan atau integrasi
  - Pengujian yang menggabungkan pengujian unit dan pengujian sistem yang dilakukan serentak.

Terdapat satu lagi pengujian iaitu pengujian penerimaan yang dilakukan oleh pengguna untuk mengenalpasti segala keperluan pengguna dipenuhi atau tidak dan sistem yang dikehendaki ditepati atau tidak.

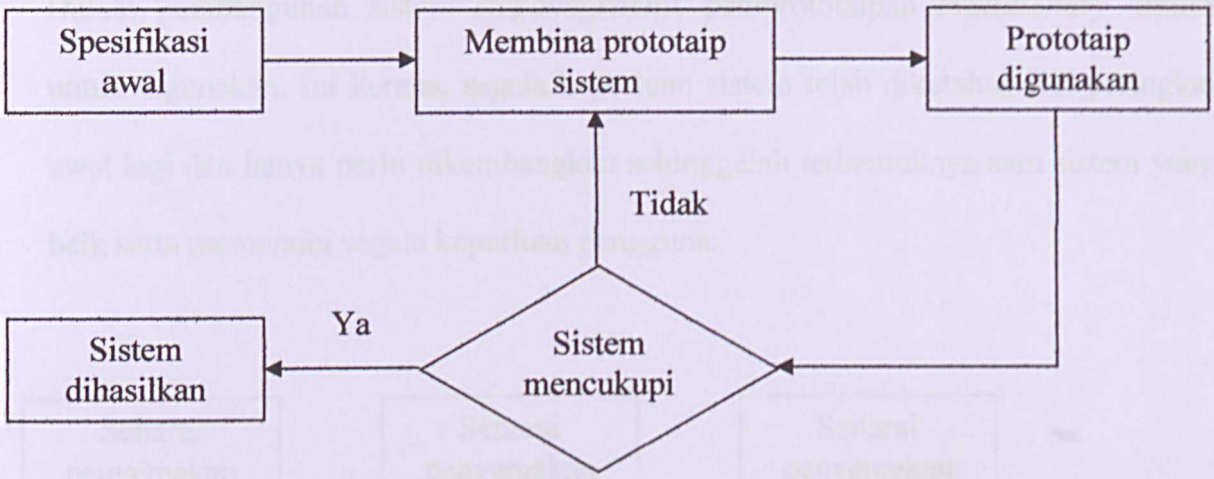
Fasa Penyelenggaraan

Fasa penyelenggaran merupakan fasa terakhir dalam pembangunan sistem. Setiap masalah yang wujud di dalam sistem akan diselenggara dengan baik supaya masalah sedemikian tidak wujud lagi pada masa akan datang. Penyelenggaraan hendaklah dilakukan dari semasa ke semasa iaitu dari awal pembangunan sistem sehinggalah sistem telah digunakan oleh pengguna.

3.4 PEMPROTOTAIPAN

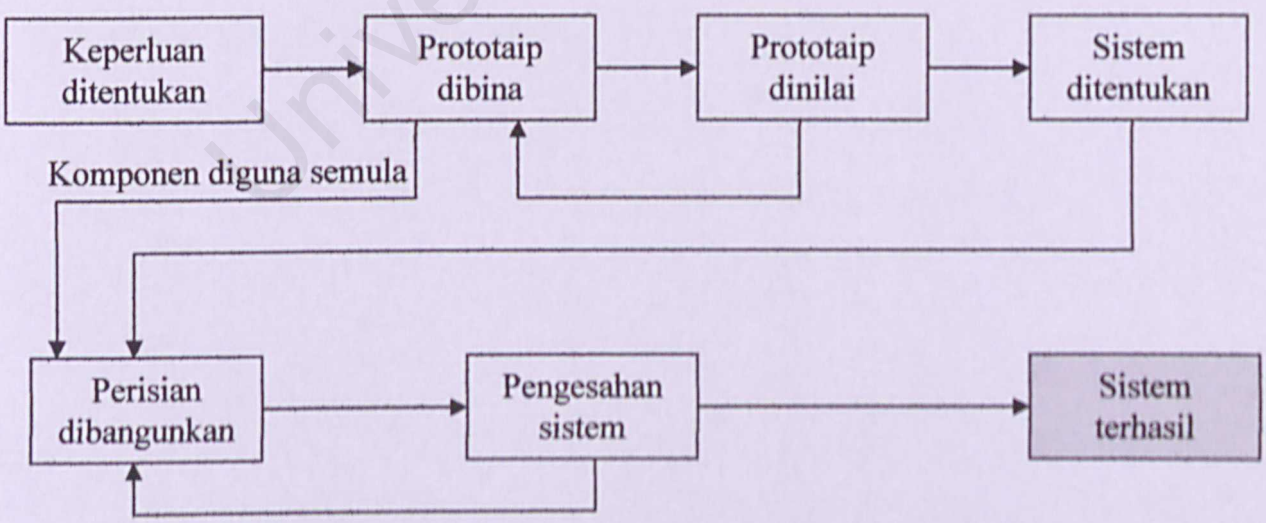
Tujuan utama pemprototaipan ialah untuk meningkatkan ketepatan perspektif pembangun sistem berdasarkan keperluan pengguna. Pemprototaipan ialah berdasarkan kepada idea membangunkan impementasi di peringkat awal di mana mendedahkan proses implementasi bagi mendapatkan maklum balas daripada pengguna. Proses ini akan diulang sehinggalah sistem lengkap dan berjaya. Terdapat dua jenis pemprototaipan, iaitu :-

- Pemprototaipan *Evolutionary*
  - objektifnya adalah untuk bekerja dengan pengguna dan memperkembangkan satu sistem daripada spesifikasi yang telah dirancangkan. Haruslah bermula dengan pemahaman keperluan yang baik.



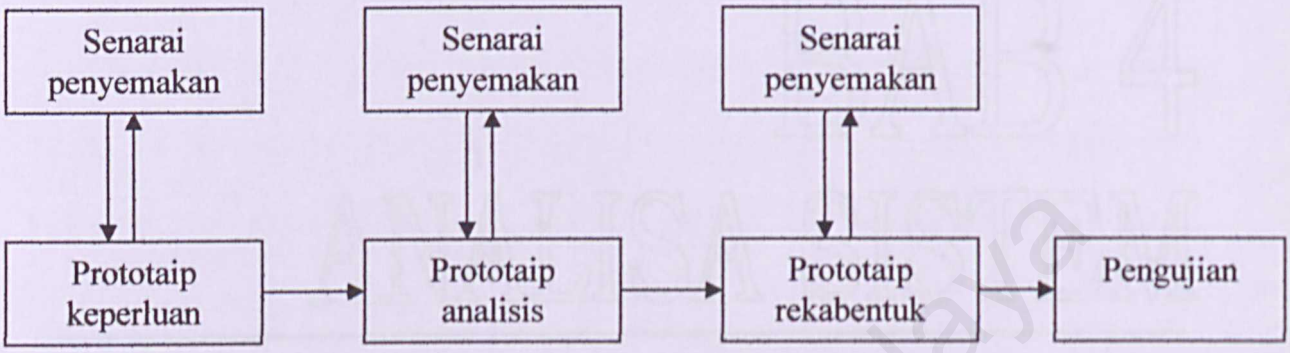
Rajah 3.2 : Pemprototaipan *Evolutionary*

- Pemprototaipan *Throw-away*
  - objektifnya ialah untuk memahami keperluan sistem. Haruslah bermula dengan pemahaman keperluan pengguna yang rendah.



Rajah 3.3 : Pemprototaipan *Throw-away*

Dalam pembangunan sistem *steganography*, pemprototaipan *evolutionary* dipilih untuk digunakan. Ini kerana, segala keperluan sistem telah diketahui dari peringkat awal lagi dan hanya perlu dikembangkan sehinggalah terbentuknya satu sistem yang baik serta memenuhi segala keperluan pengguna.



Rajah 3.4 : Model Pemprototaipan bersama Model Air Terjun

BAB 4
ANALISA SISTEM

4.1 SPESIFIKASI KEPERLUAN SISTEM

4.2 KEPERLUAN FUNGSIAN

4.3 KEPERLUAN BUKAN FUNGSIAN

4.4 KEPERLUAN PERISIAN

4.5 KEPERLUAN SISTEM PENGENDALIAN

4.6 KEPERLUAN PERKAKASAN

BAB 4

ANALISA SISTEM

4.1 SPESIFIKASI KEPERLUAN SISTEM

Dalam menghasilkan sesuatu sistem yang baik, setiap keperluan sistem hendaklah dikenalpasti dan diketahui terlebih dahulu. Ini penting agar setiap yang dikehendaki di dalam sistem dapat dipenuhi. Spesifikasi keperluan sistem terbahagi kepada dua bahagian utama, iaitu :-

- Keperluan fungsian
- Keperluan bukan fungsian

Kedua-dua keperluan ini memainkan peranan yang penting dalam menghasilkan sesuatu sistem.

Keperluan fungsian ditakrifkan sebagai fungsi-fungsi utama yang terdapat di dalam sistem dan bagaimana sistem dapat bertindak balas dengan baik samada dengan pengguna, pembangun dan sistem itu sendiri. Selain itu, keperluan fungsian juga menspesifikasikan setiap sistem yang dihasilkan berkebolehan berfungsi dengan baik terutama sekali terhadap input dan output yang dihasilkan. Keperluan fungsian biasanya dikendalikan ketika fasa analisa sistem dijalankan.

Keperluan bukan fungsian pula ditakrifkan sebagai ciri-ciri lain yang mesti terdapat di dalam sistem serta halangan-halangan terhadap fungsi yang terdapat oleh sistem tersebut. Keperluan bukan fungsian ini biasanya dikendalikan ketika fasa rekabentuk sistem dibangunkan.

4.2 KEPERLUAN FUNGSIAN

Keperluan fungsian secara amnya menceritakan fungsi-fungsi utama yang terdapat di dalam sistem yang akan dibangunkan dan juga yang dikehendaki oleh pengguna. Keperluan fungsian juga menerangkan interaksi antara sistem dengan persekitarannya dan menakrifkan sifat-sifat sesebuah sistem. Bagi sistem *steganography*, terdapat dua modul utama iaitu modul penyembunyian teks atau fail dan juga modul pembacaan teks atau fail. Model penyembunyian teks atau fail direka khas untuk pengirim menyembunyikan teks atau fail sebelum dihantar kepada penerima melalui emel manakala modul pembacaan teks atau fail pula direka khas kepada penerima untuk membaca data yang disembunyikan yang diterima oleh pengirim. Kedua-dua modul ini merangkumi beberapa modul kecil yang bertindak sebagai keperluan fungsian sistem *steganography*. Berikut adalah keperluan-keperluan fungsian yang terdapat dalam sistem *steganography*, iaitu :-

Modul Penyembunyian Teks atau Fail

1. **Membuka fail imej**

   Pembukaan fail imej digunakan untuk memilih imej yang diperlukan bagi tujuan menyembunyikan teks atau fail disebaliknya. Imej yang dipilih adalah berdasarkan pada format bitmap (.bmp).

2. **Pemilihan teks atau fail**

Pengirim akan memasukkan maklumat yang berbentuk teks atau memilih fail untuk disembunyikan disebalik imej. Teks yang dimasukkan mempunyai had yang tertentu agar tidak terlalu panjang dan fail yang dipilih adalah berdasarkan pada format teks (.txt).

3. **Pengesahan kata laluan**

Pengirim perlu memasukkan kata laluan yang tertentu ke dalam sistem. Ini penting kerana, kata laluan yang digunakan oleh pengirim akan turut digunakan oleh penerima untuk membaca teks atau fail yang dihantar. Kata laluan ini hanya diketahui oleh pengirim dan penerima sahaja agar setiap teks atau fail yang dihantar tidak dapat dibaca oleh orang lain.

4. **Penyembunyian teks atau fail**

Proses penyembunyian dilaksanakan berdasarkan teks yang dimasukkan atau fail yang dipilih oleh pengirim.

5. **Penyimpanan**

Selepas penyembunyian disebalik imej berjaya dilakukan, imej tersebut akan disimpan sebagai fail imej yang baru atau menggantikan fail imej yang lama. Kemudian, pengirim akan menggunakan fail imej ini untuk dihantar kepada penerima melalui emel.

Modul Pembacaan Maklumat atau Fail

1. **Membuka fail imej**

   Fail imej yang diterima daripada pengirim akan dibuka untuk membaca teks atau fail dalam proses yang berikutnya.

2. **Pengesahan kata laluan**

   Penerima perlu memasukkan kata laluan yang sama dengan kata laluan pengirim agar dapat membaca teks atau fail disebalik imej. Kata laluan yang salah akan menyebabkan penerima tidak boleh membaca teks atau fail yang disembunyikan.

3. **Pemisahan data daripada imej**

   Selepas fail imej dipilih, pemisahan data daripada imej akan dilakukan. Data akan dipisahkan daripada imej agar penerima boleh membaca data yang tersembunyi disebalik imej tersebut.

4. **Paparan teks atau penyimpanan fail**

   Teks yang tersembunyi akan dipaparkan atau fail yang didapati akan disimpan terlebih dahulu sebelum dapat membacanya.

4.3 KEPERLUAN BUKAN FUNGSIAN

Keperluan bukan fungsian merupakan satu tindak balas sistem dalam menghasilkan sistem yang berkualiti tinggi dan berkesan serta dapat menyelesaikan halangan-halangan yang wujud di dalam sistem. Keperluan bukan fungsian juga menerangkan sifat-sifat dan ciri-ciri sesebuah sistem yang dibangunkan. Dalam erti kata lain, keperluan yang seharusnya ada dalam sesebuah sistem. Bagi sistem *steganography* yang dibangunkan, terdapat beberapa keperluan bukan fungsian yang dijangkakan dan diperolehi, iaitu :-

1. **Mesra pengguna**

   Sistem *steganography* yang dibangunkan adalah satu sistem yang mesra pengguna, mudah difahami dan senang digunakan. Ini memudahkan pengguna untuk berinteraksi dengan sistem yang dibangunkan. Pengguna akan lebih senang memahami penggunaan dan perjalanan sistem dengan lebih cepat. Sebarang masalah lebih senang diatasi dengan adanya sistem yang lebih mesra pengguna.

2. **Kebolehan kepercayaan yang tinggi**

   Sistem ini boleh dipercayai kerana mempunyai ciri-ciri keselamatan yang baik bagi mengelakkan sebarang pencerobohan terhadap teks atau fail yang disembunyikan. Ciri-ciri keselamatan ini termasuklah kata laluan dan proses penyembunyian data yang digunakan.

3. **Kebolehselenggaraan**

Setiap modul sistem akan dipecahkan kepada modul-modul kecil untuk memudahkan penyelenggaraan sistem yang dibangunkan. Penyelenggaraan modul yang mudah akan dapat mengatasi masalah yang wujud di dalam sistem dengan lebih cepat. Ini memberi kebaikan kepada pembangun sistem untuk menyelenggara sistem sekiranya terdapat keperluan yang tidak memenuhi keperluan pengguna. Selain itu, sistem yang dibangunkan juga lebih mudah untuk ditingkatkan pada masa akan datang disebabkan penyelenggaraan yang terurus dan tersusun.

4. **Rekabentuk dan kestabilan paparan**

Penekanan dan penelitian haruslah diberikan terhadap rekabentuk dan kestabilan paparan dalam menghasilkan satu persembahan sistem yang baik dan menarik. Penekanan haruslah diberikan pada kualiti dan keringkasan teks yang digunakan. Teks yang digunakan di dalam sistem mestilah mudah dibaca dan menarik perhatian pengguna. Teks yang ringkas juga akan menyebabkan pengguna tidak mengambil masa yang terlalu lama untuk memahami apa yang dimaksudkan dan teks tersebut merupakan isi-isi penting yang berkaitan dengan sistem. Selain itu, penekanan juga harus diberikan pada pemilihan warna yang digunakan pada sistem. Warna latar belakang dan tulisan yang digunakan mestilah mengikut kesusuaian sistem dan tidak terlalu kontra sehingga menimbulkan kebosanan kepada pengguna yang menggunakannya. Kestabilan paparan yang diwujudkan adalah penting bagi memastikan setiap elemen-elemen yang ada di dalam sistem dapat berfungsi dengan baik bukan sahaja pada kali pertama tetapi untuk setiap masa.

5. **Mudah dan konsisten**

Aturcara pengekodan yang digunakan untuk membangunkan sistem *steganography* ini adalah mudah dan tidak kompleks. Sehubungan itu, penyelenggaraan lebih mudah dilakukan seperti membaik pulih semula sistem yang dibangunkan.

6. **Kebolehan pengubahsuaian**

Setiap sistem mempunyai had tempoh masa yang tertentu bagi membolehkan sistem mengikut perkembangan teknologi yang lebih baru. Kebolehan pengubahsuaian sistem memberi kelebihan kepada sistem untuk dipertingkatkan. Persekitaran baru dan sumber yang digunakan hendaklah lebih mudah untuk diaplikasikan ke dalam sistem yang dibangunkan.

7. **Kawalan capaian yang ketat**

Kawalan capaian yang ketat penting dalam sesuatu sistem. Hanya pengguna yang berdaftar sahaja iaitu pengguna yang mengetahui kata laluan pengirim sahaja akan dapat membaca teks atau fail yang dihantar.

8. **Masa maklum balas**

Masa maklum balas yang diperuntukkan dalam sistem hendaklah berada dalam kadar masa yang bersesuaian pada setiap aktiviti sistem. Ini berhubung rapat dengan maklumat yang dipaparkan pada setiap aktiviti. Ini kerana, maklumat yang dipaparkan hendaklah ringkas dan bersesuaian agar tidak mengambil masa maklum balas yang lama pada setiap aktiviti.

4.4 KEPERLUAN PERISIAN

Bagi membangunkan sesuatu sistem, pemilihan perkakasan adalah amat dititik beratkan. Ini kerana, perkakasan yang bersesuaian dengan sistem yang dibangunkan akan menghasilkan sistem yang baik perjalanannya. Bagi membangunkan sistem *steganography*, perisisan *Microsoft Visual Basic 6.0* digunakan dalam merekabentuk antaramuka.

4.4.1 MICROSOFT VISUAL BASIC 6.0

Visual Basic 1.0 direvolusikan oleh pembangunan *windows* dengan mengurangkan halangan dan rintangan dan menghasilkan sebilangan besar pengaturcara lebih produktif daripada sebelum ini. Daripada sejarah ini, *Visual Basic 6.0* dibangunkan dengan menawarkan pemahaman yang mendalam mengenai tugas seorang pengaturcara sebagai manusia yang berkebolehan membaca setiap sintaks, antaramuka pengguna yang lebih menarik dan perkakasan yang mencepatkan pembangunan *Microsoft. Visual Basic 6.0* mengambil kelebihan pada kemudahan pembangunan dengan melampaui kedudukan asal, sementara melakukan penambahan baru yang membenarkan pelbagai kategori pengaturcara menggunakannya, daripada peringkat permulaan sehingga ke pembangun korporat yang berpengalaman untuk membangunkan aplikasi-aplikasi bagi *windows*, laman web dan peranti mudah.

Selain itu, terdapat juga kemudahan perpustakaan (DLL) dan fungsi-fungsi terbina dalam (*built-in-functions*). Ini membenarkan pengaturcara mencipta perpustakaan sendiri dalam bahasa baru seperti bahasa C++ untuk dilarikan bersama-

sama dengan perisian. Kebanyakan pengaturcara lebih gemar menggunakan *Visual Basic 6.0* untuk merekabentuk antaramuka dan bahasa C++ sebagai enjin kepada sistem. *Visual Basic 6.0* juga mempunyai mutu persembahan yang baik dan mengamalkan konsep pengaturcaraan berorientasikan objek (OOP) yang mempunyai kelebihan kelas, perwarisan dan polimofisme yang juga membolehkan tugas-tugas pembangunan dimulakan semula dan dilanjutkan dengan lebih cekap.

Terdapat beberapa kelebihan yang boleh didapati pada *Visual Basic 6.0*, antaranya ialah :-

- Struktur bahasa pengaturcaraan yang digunakan ialah mudah dan sama seperti had perlaksanaan.
- Bukan sahaja dikenali sebagai bahasa pengaturcaraan tetapi juga sebagai satu penyepaduan, persekitaran pembagunan interaktif (IDE).
- VB.IDE digunakan untuk menyokong *Rapid application development*, yang memudahkan pembangunan antaramuka pengguna dan menguhubungkannya kepada fungsi-fungsi yang bertanggungjawab.
- VB menghasilkan satu interaktif yang komprehensif dan konteks-sensitif sistem bantuan atas talian.
- VB ialah satu komponen gabungan bahasa di mana disetalakan kepada model komponen objek *Microsoft* (COM).
- COM boleh ditulis dalam pelbagai bahasa yang kemudiannya digabungkan menggunakan VB.
- COM boleh dibenamkan atau dihubungkan kepada aplikasi antaramuka pengguna dan juga disimpan ke dalam dokumen.

4.5 KEPERLUAN SISTEM PENGENDALIAN

Sistem pengendalian memainkan peranan penting agar sistem dapat dibangunkan dan digunakan dengan baik. Bagi membangunkan sistem *steganography*, sistem pengendalian yang digunakan ialah *Microsoft Windows XP Professional*.

4.5.1 *MICROSOFT WINDOWS XP PROFESSIONAL*

Microsoft Windows XP Professional dipilih sebagai sistem pengendalian utama bagi sistem *steganography* kerana terdapat pelbagai kemudahan yang mudah digunakan dan kestabilannya pada setiap kali sistem dibangunkan. Ini dibuktikan dengan pelbagai sistem yang sedia ada di pasaran. Kestabilan yang terdapat pada *Windows XP Professional* adalah ciri-ciri yang amat penting dan dititik beratkan yang boleh membawa kepada keberkesanan pada sistem *steganography*. Penggunaan senibina 32-bit dapat mengurangkan peluang untuk setiap aplikasi gagal dilaksanakan dan juga *reboots* yang tidak dirancang.

Selain itu, ciri-ciri mesra pengguna yang terdapat pada *Windows XP Professional* juga menjadikannya sebagai sistem pengendalian yang kian menjadi pilihan pembangun sistem. Ini kerana, pengguna lebih senang memahami dan menggunakannya tanpa menghadapi sebarang masalah. Sistem pengendalian ini juga memberi kelebihan kepada pengguna-pengguna yang sebelum ini pernah menggunakan versi-versi *Microsoft* sebelum *Windows XP Professional* dibangunkan. Ini kerana, persekitaran dan keadaan setiap versi sebelum ini mempunyai persamaan antara satu sama lain samada dari segi aplikasinya dan penggunaannya. Sehubungan

itu, pengguna-pengguna yang belum pernah menggunakannya dapat mempelajarinya dengan lebih mudah.

Windows XP Professional juga lebih menekankan kepada penggunaan grafik dan warna yang menarik. Keadaan ini akan memudahkan sesuatu sistem dibangunkan kerana mengambil kelebihan pada ciri tersebut. Di samping itu juga, setiap fungsi yang terdapat di dalamnya dapat difahami dengan mudah.

4.6 KEPERLUAN PERKAKASAN

Jadual 4.1 : Jadual keperluan perkakasan yang diperlukan sistem *steganography*.

Perkakasan	Minima	Cadangan
Pemproses	Pentium II 450MHz	Pentium III 600MHz
RAM (Memori)	96 MB	128 MB
Cakera Keras	10GB	40GB
Monitor	VGA	SVGA
Paparan Warna	256 warna	256 warna
Peranti Input	Tetikus Papan kekunci	Tetikus Papan kekunci CD-ROM / DVD-ROM
Sistem Pengendalian	Windows 2000	Windows XP Professional

BAB 5
REKABENTUK SISTEM

5.1 REKABENTUK SISTEM

5.2 GAMBARAJAH PENGALIRAN DATA (DFD)

5.3 REKABENTUK SISTEM STEGANOGRAPHY

5.4 GAMBARAJAH KONTEKS PENGALIRAN DATA

5.5 CARTA ALIR SISTEM STEGANOGRAPHY

5.6 REKABENTUK ANTARAMUKA SISTEM *STEGANOGRAPHY*

BAB 5

REKABENTUK SISTEM

5.1 REKABENTUK SISTEM

Rekabentuk sistem adalah satu proses penterjermahan keperluan yang telah dinyatakan pada fasa sebelum ini kepada bentuk persembahan sistem. Bentuk persembahan sistem ini juga dikenali sebagai rekabentuk antaramuka yang terdapat pada sesuatu sistem. Antaramuka sistem ini memainkan peranan yang penting kepada pengguna untuk mengendalikan sistem dan memahami fungsi sesuatu sistem. Sistem yang mempunyai antaramuka yang menarik dan senang difahami akan menjadikan pengguna lebih mudah memahami fungsi sistem yang dibangunkan dan dapat mewujudkan satu komunikasi yang berkesan antara pengguna dan sistem. Sistem yang baik mempunyai hasil rekabentuk antaramuka yang berkualiti dan sentiasa mengekalkan kestabilan pada setiap antaramuka. Sebaliknya, antaramuka yang kurang menarik dan sukar untuk difahami akan menyebabkan daya tarikan pengguna ke atas sistem semakin berkurangan. Justeru itu, rekabentuk antaramuka sistem haruslah meliputi dan merangkumi tahap kepuasan pengguna.

Dalam menentukan kualiti ke atas setiap rekabentuk antaramuka sistem, pengguna akan bertindak sebagai penilai utama selain pembangun sistem sendiri samada baik atau tidak. Ini kerana, setiap sistem yang dibangunkan adalah berdasarkan kepada keperluan pengguna itu sendiri. Sehingga ke hari ini, antaramuka yang masih mendapat perhatian pembangun sistem ialah antaramuka yang berasaskan teks. Ini kerana, penggunaan teks akan menjadikan fungsi sesuatu sistem

lebih senang difahami oleh pengguna yang menggunakannya. Walau bagaimanapun, rekabentuk antaramuka teks kini mula beralih ke rekabentuk antarmuka pengguna grafik (*GUI*). Antaramuka pengguna grafik mempunyai ciri-ciri yang berlainan, di mana lebih cenderung ke arah penggunaan grafik. Penggunaan grafik yang banyak akan menimbulkan daya tarikan kepada pengguna untuk menggunakan sistem tersebut. Antaramuka ini mula mendapat perhatian di kalangan pembangun sistem kerana terdapat beberapa kelebihan, antaranya ialah :-

- Antaramuka pengguna grafik adalah hasil gabungan antara teks dan grafik di mana pemahaman mengenai mesej yang hendak disampaikan oleh sistem akan lebih mudah tercapai terutama sekali kepada pengguna.
- Masa yang diambil untuk berinteraksi pada setiap antaramuka juga akan menjadi lebih cepat dan tidak perlu mengambil masa yang lama. Keadaan ini akan menyebabkan pengguna akan tidak rasa cepat jemu dengan sistem yang digunakan.
- Antaramuka pengguna grafik mementingkan padanan antara grafik dan warna yang digunakan untuk menarik minat pengguna menggunakannya sekaligus dapat mengalih perhatian kepada sistem yang baru.
- Mempunyai tetingkap yang banyak untuk perpindahan dari satu proses ke satu proses yang berikutnya. Pengguna masih boleh melakukan pengubahsuaian pada tetingkap yang sebelumnya walaupun sudah berada pada tetingkap yang selepasnya.

- Pengguna lebih senang memahami fungsi dan kehendak sistem yang sebenarnya. Pelbagai lapisan pengguna boleh menggunakannya dengan hanya berpandukan antaramuka tanpa sebarang pembelajaran komputer termasuklah golongan kanak-kanak. Pelbagai perisian yang berasaskan antaramuka pengguna grafik telah dibangunkan untuk golongan kanak-kanak.

5.2 GAMBARAJAH PENGALIRAN DATA (DFD)

Gambarajah pengaliran data (*DFD*) ialah satu model proses yang digunakan untuk menggambarkan perjalanan data melalui satu sistem atau proses yang dipersembahkan oleh sistem. Selain itu, gambarajah pengaliran data juga boleh digambarkan sebagai perwakilan satu sistem pada setiap peringkat secara terperinci menggunakan simbol-simbol yang menunjukkan pengaliran data, simpanan data, proses data dan juga sumber atau destinasi data.

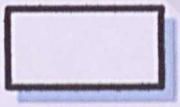
Tujuan utama gambarajah pengaliran data dihasilkan ialah untuk menunjukkan hubungan yang semantik antara pengguna dan pembangun sistem. Objektif utama gambarajah pengaliran data secara amnya ialah untuk memahami model sebenar sesuatu sistem. Gambarajah pengaliran data disokong oleh pelbagai teknik struktur analisa sistem yang lain seperti gambarajah struktur data, kamus data dan sebagainya. Selain itu, gambarajah pengaliran data mempunyai persamaan dengan carta gelembung, graf penukaran dan model proses.

Terdapat beberapa kelebihan yang didapati pada gambarajah pengaliran data, iaitu :-

- Gambarajah pengaliran data boleh beroperasi secara selari iaitu beberapa proses boleh dilakukan secara serentak pada satu masa.
- Gambarajah pengaliran data menunjukkan secara terperinci setiap perjalanan data melalui sistem di mana setiap proses dapat difahami dan diteliti dengan jelas satu persatu.
- Proses-proses yang terdapat pada gambarajah pengaliran data boleh mempunyai pelbagai pemasaan seperti hari dan minggu.
- Gambarajah pengaliran data menyokong pemikiran sistem iaitu aplikasi teori sistem formal dan konsep untuk menyelesaikan masalah sistem.

5.2.1 SIMBOL-SIMBOL PADA DFD

I. Simbol entiti



- Mewakili sumber data kepada sistem atau destinasi data daripada sistem.
- Bertindak sebagai orang luar, unit organisasi atau sistem organisasi yang berinteraksi dengan sistem.
- Menakrifkan skop atau sempadan setiap sistem yang dimodelkan.

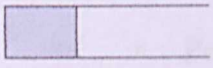
II. Simbol pengaliran data

- Menunjukkan pergerakan data dari satu proses ke proses yang lain.

- Mewakili pergerakan data yang diinputkan kepada setiap proses atau data yang dihasilkan daripada proses.
- Digunakan untuk mewakili pembacaan, pembuangan, pembinaan atau pengemaskinian data dalam sesuatu fail atau pangkalan data.

III. Simbol simpanan data

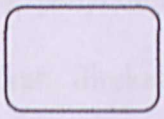
- Mewakili data yang tidak bergerak.
- Sinonim dengan fail atau pangkalan data.



- Menunjukkan data pada ketika berehat sebelum melakukan proses lain.
- Boleh bertindak samada sebagai orang, tempat, objek, acara atau konsep yang digunakan.

IV. Simbol proses

- Mewakili aktiviti yang memanipulasikan data iaitu gabungan atau susunan semula.



- Menunjukkan proses kerja yang dipersembahkan oleh satu sistem dalam bertindak balas kepada data yang akan tiba.
- Sinonim kepada jelmaan.

5.3 REKABENTUK SISTEM *STEGANOGRAPHY*

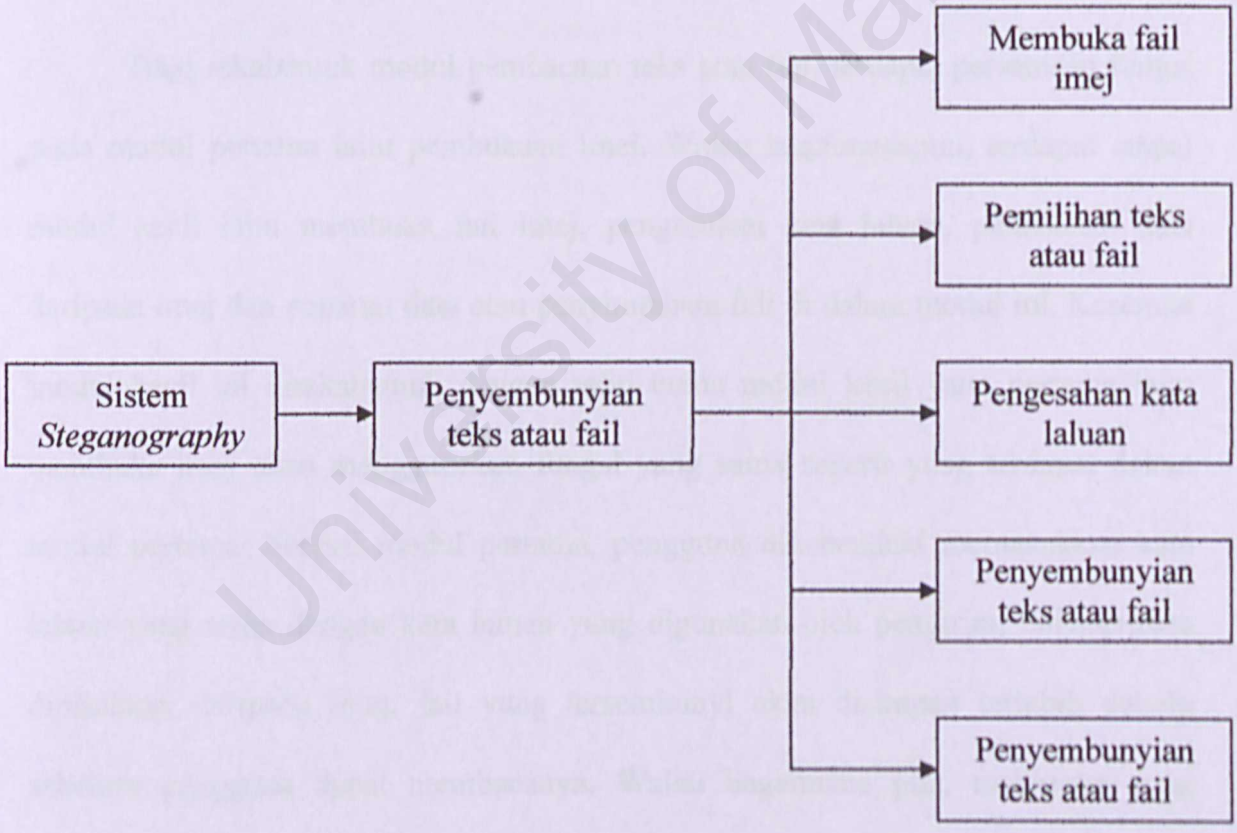
Rekabentuk sistem *steganography* adalah terjemahan daripada keperluan sistem yang telah dinyatakan pada fasa sebelum ini kepada persembahan sistem. Persembahan sistem ini akan digunakan oleh pembangun sistem dan juga pengguna sistem. Dalam menghasilkan rekabentuk sistem *steganography*, keperluan sistem dikaji semula agar menepati kehendak pengguna. Sistem *steganography* dibangunkan peringkat demi peringkat dan mengikut kesesuaian modul. Modul yang besar akan dipecahkan kepada beberapa modul kecil dalam fasa sebelum ini. Modul dan modul-modul kecil yang lebih senang akan dibangunkan terlebih dahulu dan dituruti dengan modul dan modul kecil yang kompleks. Terdapat dua modul utama iaitu :-

- Penyembunyian teks atau fail
- Pembacaan teks atau fail

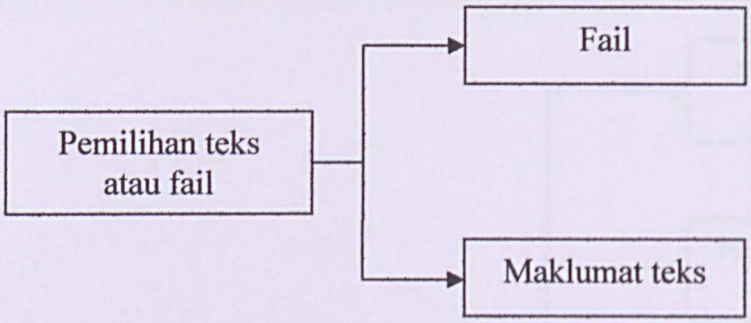
5.3.1 MODUL PENYEMBUNYIAN TEKS ATAU FAIL

Modul penyembunyian teks atau fail telah dibahagikan kepada beberapa modul kecil iaitu membuka fail imej, pemilihan teks atau fail, pengesahan kata laluan, penyembunyian teks atau fail dan juga penyimpanan. Kesemua modul kecil ini akan direkabentuk mengikut kesesuaian sistem dan setiap modul kecil ini mempunyai satu atau dua fungsi. Bagi memulakan penyembunyian teks atau fail, pengguna dikehendaki membuka satu fail imej yang berformat bitmap sahaja. Dalam modul kecil pemilihan teks atau fail, pengguna boleh memilih samada menggunakan fail untuk disembunyikan atau maklumat yang berbentuk teks. Sekiranya pengguna

memilih fail untuk disembunyikan, pengguna akan diminta untuk memilih fail berformat .txt sahaja daripada komputer atau peranti luaran yang lain, dan sekiranya pengguna memilih untuk menggunakan maklumat yang berbentuk teks, pengguna akan diminta memasukkan teks pada ruang teks yang disediakan dan tidak boleh melebihi had yang telah ditetapkan. Sebelum melakukan proses penyembunyian, pengguna akan diminta memasukkan kata laluan yang tertentu untuk keselamatan data. Selepas itu, modul kecil penyembunyian teks atau fail akan dilaksanakan. Fail imej yang telah disembunyikan dengan teks atau fail akan disimpan sebelum dihantar kepada penerima.



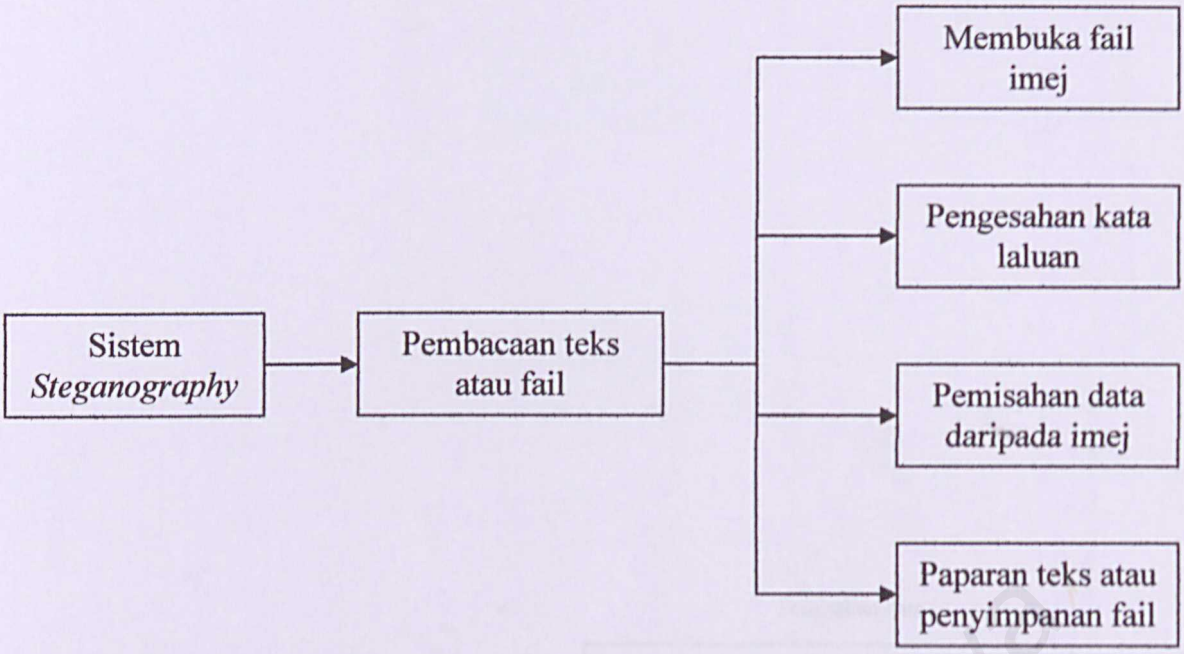
Rajah 5.1 : Hierarki modul penyembunyian teks atau fail



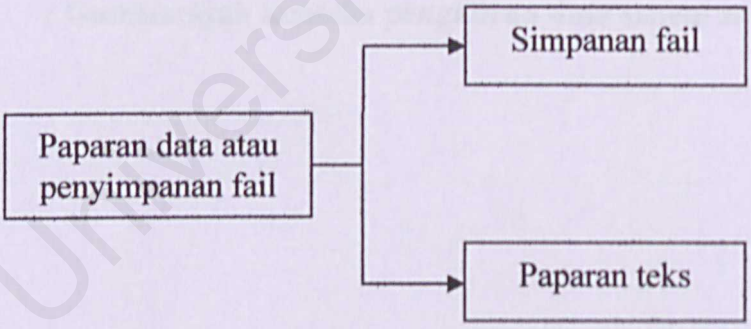
Rajah 5.2 : Pilihan pada modul kecil penyembunyian teks atau fail

5.3.2 MODUL PEMBACAAN MAKLUMAT ATAU FAIL

Bagi rekabentuk modul pembacaan teks atau fail, terdapat persamaan fungsi pada modul pertama iaitu pembukaan imej. Walau bagaimanapun, terdapat empat modul kecil iaitu membuka fail imej, pengesahan kata laluan, pemisahan data daripada imej dan paparan data atau penyimpanan fail di dalam modul ini. Kesemua modul kecil ini direkabentuk dengan teliti cuma modul kecil yang pertama iaitu membuka imej akan menggunakan fungsi yang sama seperti yang terdapat dalam modul pertama. Seperti modul pertama, pengguna dikehendaki memasukkan kata laluan yang sama dengan kata laluan yang digunakan oleh pengirim. Selepas data dipisahkan daripada imej, fail yang tersembunyi akan disimpan terlebih dahulu sebelum pengguna dapat membacanya. Walau bagaimana pun, maklumat yang berbentuk teks akan dipaparkan terus pada sistem.

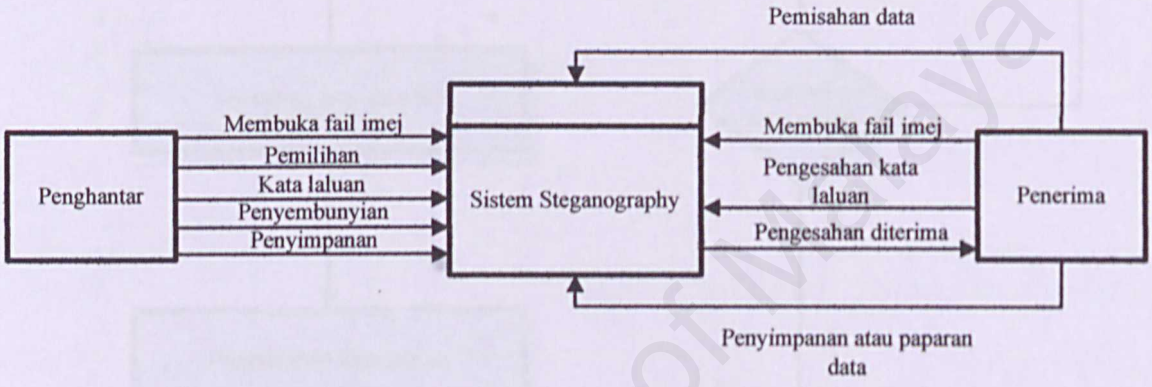


Rajah 5.3 : Hierarki modul pembacaan teks atau fail



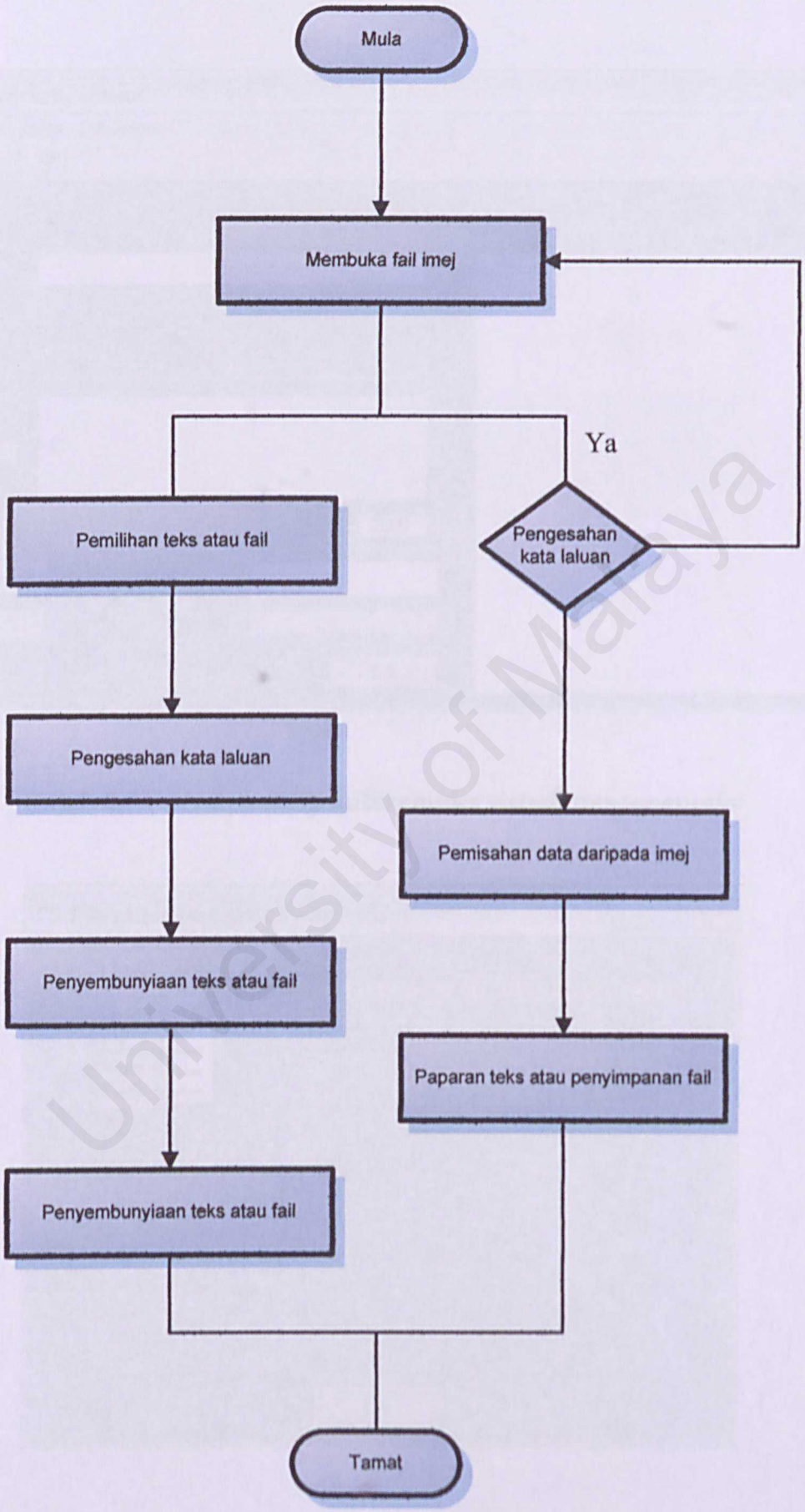
Rajah 5.4 : Dua pecahan fungsi pada modul kecil yang keempat

5.4 GAMBARAJAH KONTEKS PENGALIRAN DATA



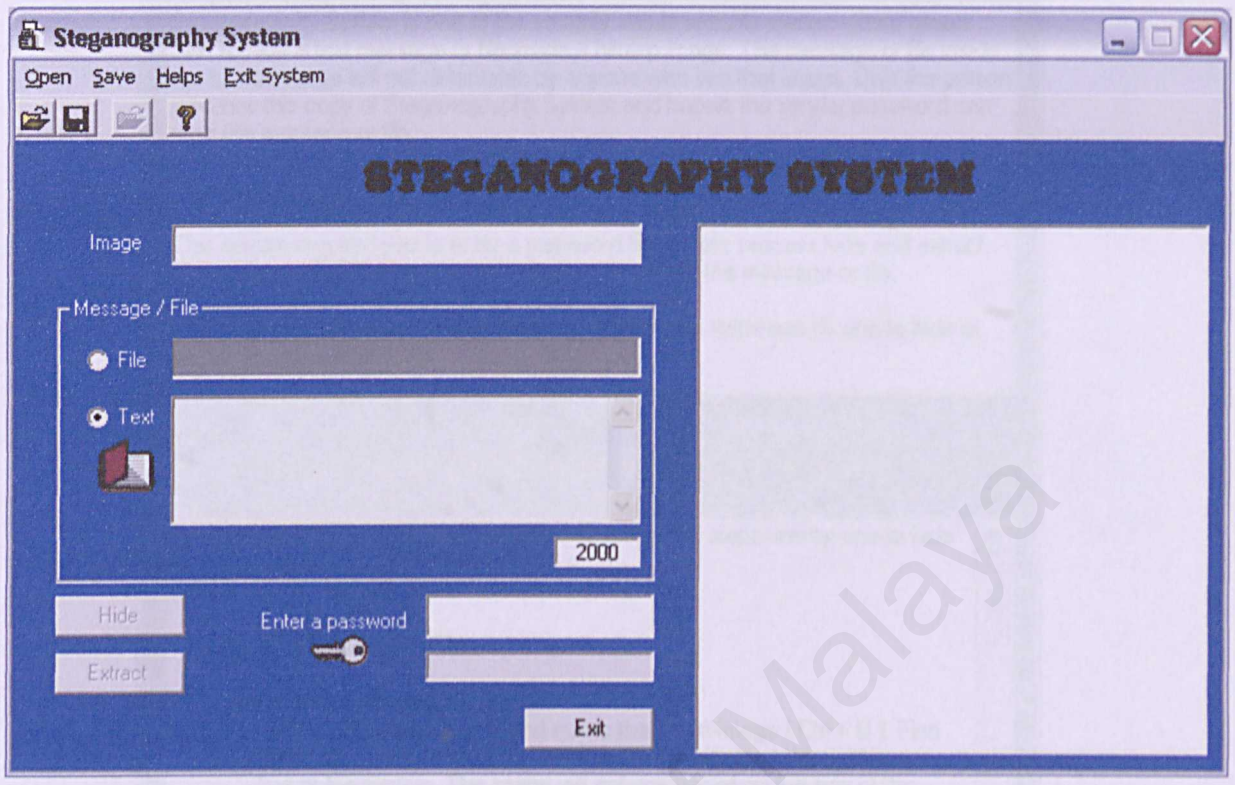
Rajah 5.5 : Gambarajah konteks pengaliran data sistem *steganography*

5.5 CARTA ALIR SISTEM *STEGANOGRAPHY*

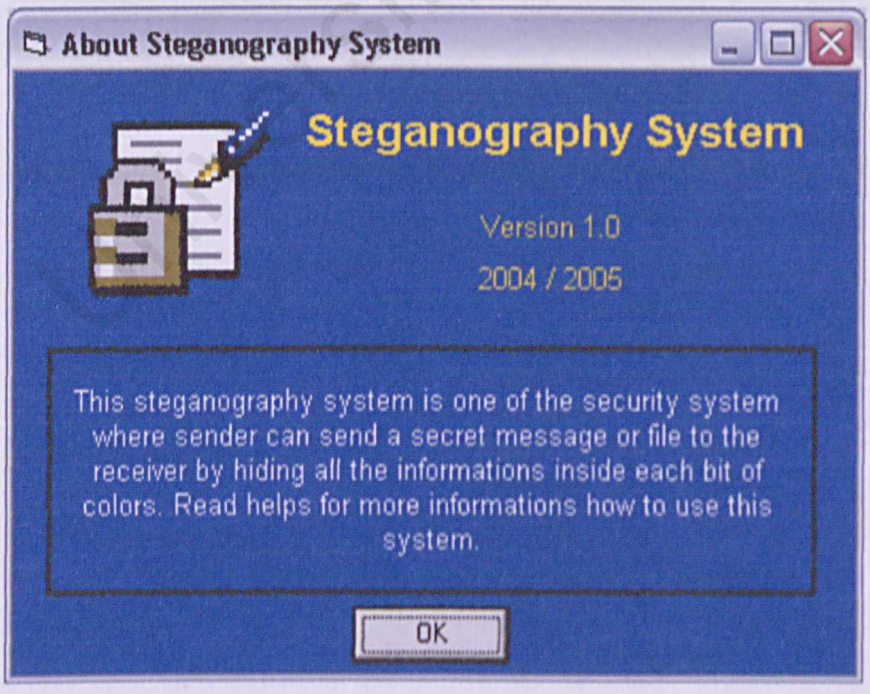


Rajah 5.6 : Carta alir bagi sistem *steganography*

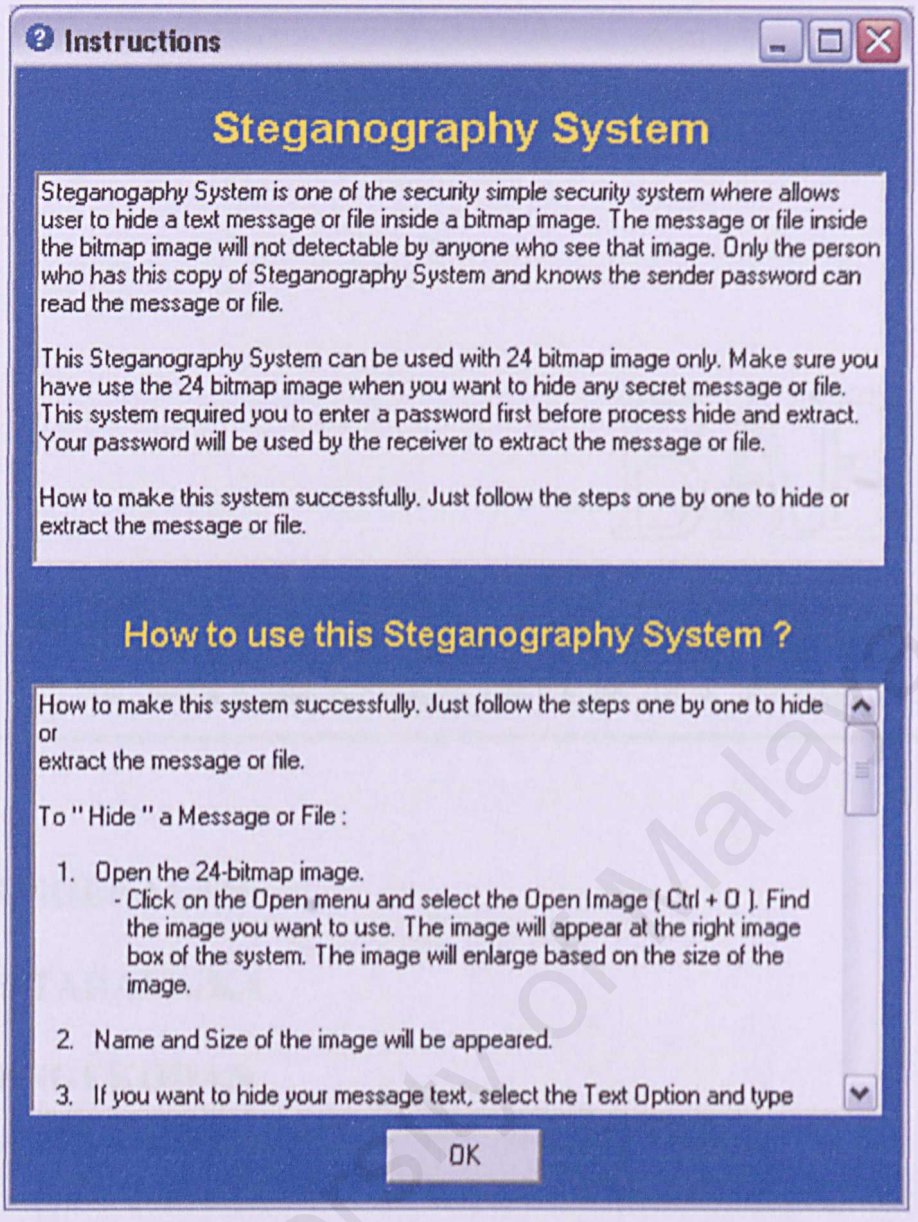
5.6 REKABENTUK ANTARAMUKA SISTEM *STEGANOGRAPHY*



Rajah 5.7 : Prototaip antaramuka sistem *steganography*



Rajah 5.8 : Prototaip antaramuka mengenai sistem *steganography*



Rajah 5.9 : Prototaip antaramuka arahan dan bantuan

BAB 6
PERLAKSANAAN SISTEM

6.1 PENGENALAN

6.2 ANTARAMUKA

6.3 PENGEKODAN

BAB 6

PERLAKSANAAN SISTEM

6.1 PENGENALAN

Bagi menghasilkan sesuatu projek atau sistem dapat berfungsi dengan baik, perlaksanaan ke atas projek atau sistem perlu dilaksanakan. Kesemua bahan yang dikumpulkan dan didapati semasa fasa analisa sistem akan diguna pakai dan digabungkan. Dalam fasa ini, dua proses utama dilakukan bagi menghasilkan sistem *steganography* dapat berfungsi mengikut keperluan yang telah ditetapkan. Dua proses utama tersebut ialah :-

- Proses perlaksanaan antaramuka
- Proses perlaksanaan pengekodan (aturcara)

Antaramuka dibina terlebih dahulu di mana dalam fasa rekabentuk sistem sebahagian antaramuka sistem telah direkabentuk. Selepas kesemua antaramuka dibina, pengekodan dilakukan bagi membolehkan sistem itu berfungsi mengikut keperluan yang telah ditetapkan dalam fasa analisa sistem. Dua proses utama ini dilaksanakan mengikut beberapa perkara yang perlu dipertimbangkan, iaitu :-

- Antaramuka -
  - antaramuka dibina dan diubahsuai mengikut kesesuaian pengguna, sistem dan bahan yang didapati.
  - pemilihan warna, teks dan corak yang sesuai.
  - menepati keperluan sistem yang telah dianalisa.

- Pengekodan -
  - pengekodan yang dilakukan mudah.
  - pengekodan dilakukan mengikut peringkat demi peringkat.
  - pengekodan mestilah mudah diselenggara bagi menepati keperluan fungsian dan bukan fungsian sistem.
- Ketahanan -
  - fungsi –fungsi dan kod yang dilaksanakan berfungsi.
  - sistem akan tergantung apabila input yang dimasukkan melebihi had julat sepatutnya.
  - sistem mampu memaparkan mesej kesalahan dan peringatan.

6.2 ANTARAMUKA

Antaramuka memainkan peranan penting dalam sesebuah sistem. Antaramuka akan menjadi panduan kepada pengguna untuk menggunakan sesuatu sistem. Ini kerana, pengguna lebih memahami sesuatu sistem dengan berpandukan pada antaramuka yang dihasilkan berbanding dengan memahami kod-kod yang digunakan. Oleh sebab itu, antaramuka perlulah mengandungi segala keperluan pengguna.

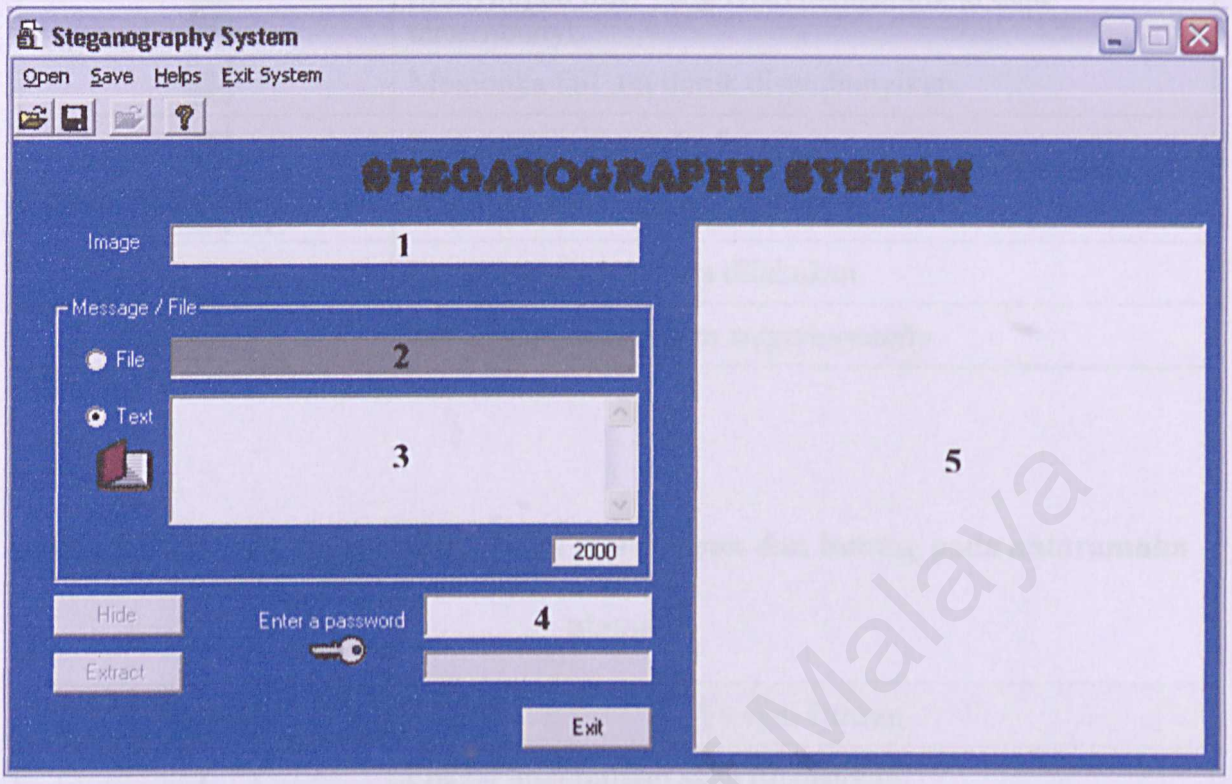
Bagi sistem *steganography*, antaramuka yang dihasilkan pada fasa rekabentuk sistem digunakan semula. Walau bagaimanapun, terdapat beberapa pengubahsuaian yang perlu dilakukan untuk memastikan antaramuka yang digunakan memenuhi segala keperluan. Antaramuka yang dihasilkan tidak terlalu komplek sehingga pengguna sukar untuk menggunakannya dan memahaminya. Ini akan menyebabkan, sistem akan digunakan dalam satu tempoh masa yang singkat.

Pemilihan warna dan teks perlu diambil kira agar bersesuaian dengan sistem yang diaplikasikan. Bagi sistem steganography, warna biru digunakan sebagai warna latar belakang bagi ketiga-tiga antaramuka sistem. Warna kuning, putih dan hitam digunakan sebagai warna teks untuk disesuaikan dengan warna latar belakang sistem. Ini penting bagi memudahkan pengguna membaca sesuatu perkataan dengan jelas dan memahami segala perkataan yang terdapat pada sistem. Walau bagaimanapun, pemilihan warna haruslah tidak terlalu kontra sehingga menimbulkan masalah kepada pengguna.

Selain itu, bagi memenuhi salah satu keperluan bukan fungsian iaitu mesra pengguna, hanya dua butang utama digunakan pada antaramuka utama sistem iaitu butang untuk proses penyembunyian dan juga butang untuk proses pemisahan data. Butang-butang lain seperti membuka imej, menyimpan imej, membuka fail dan bantuan turut digunakan bagi memastikan sesuatu proses dapat dilaksanakan. Walau bagaimanapun, butang-butang yang digunakan mempunyai persamaan dengan butang-butang yang terdapat pada perisian-perisian lain seperti *Microsoft Word*, *Microsoft Access* dan sebagainya.

Menu juga turut digunakan yang mempunyai fungsi yang sama seperti butang-butang membuka imej, menyimpan imej, membuka fail dan juga bantuan. Pengguna boleh menggunakan samada menu atau butang yang disediakan.

6.2.1 ANTARAMUKA UTAMA



Rajah 6.1 : Antaramuka utama Sistem Steganography yang dihasilkan.

Jadual 6.1 : Fungsi – fungsi utama pada menu dan butang antaramuka utama.

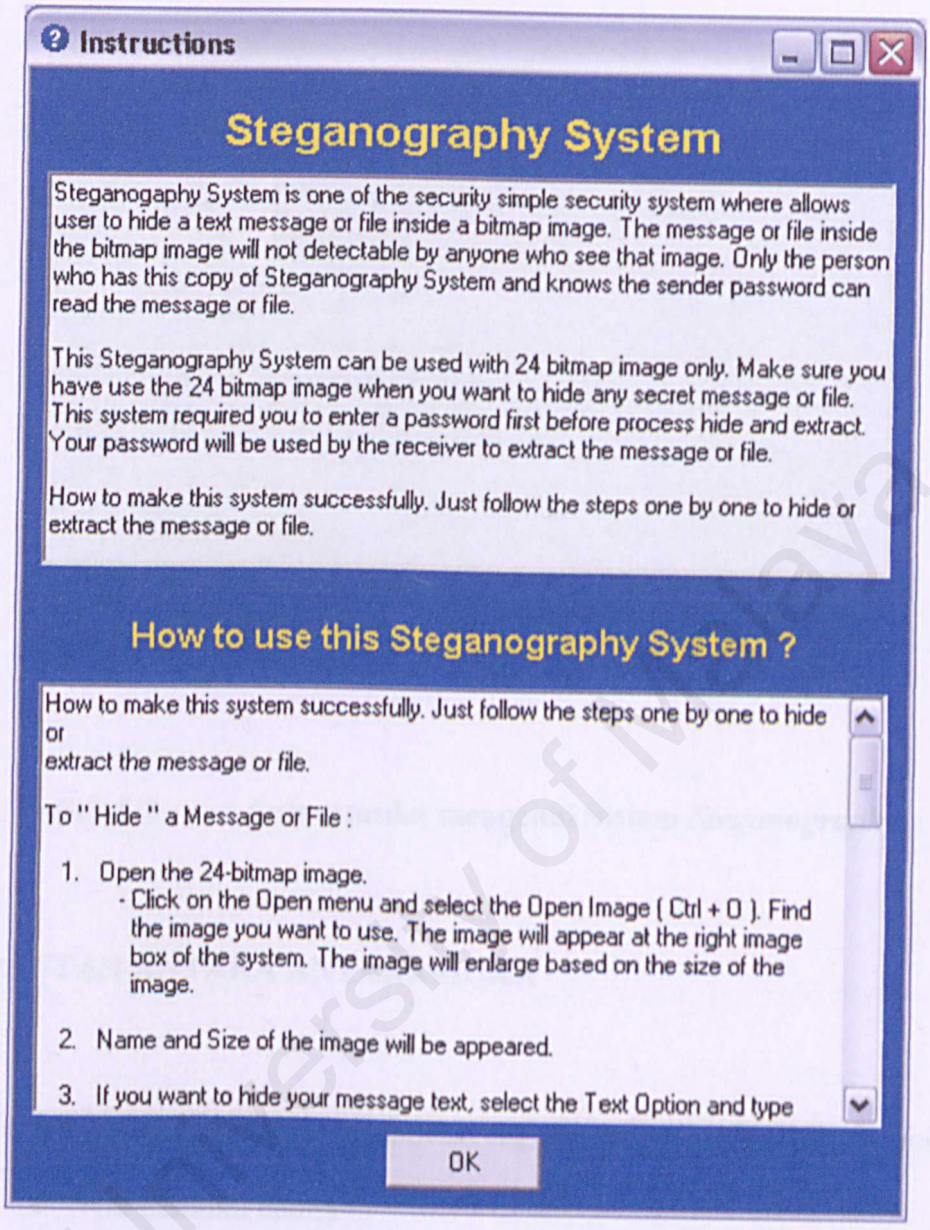
Menu dan Butang	Fungsi Utama
Open	Menu utama bagi membuka imej bitmap atau fail .txt.
Save	Menu utama bagi simpanan imej bitmap.
Helps	Menu utama bagi pautan ke antaramuka bantuan atau antaramuka mengenai sistem *steganography*.
Exit System	Keluar daripada sistem *steganography*.
Open Image Ctrl+O	Membuka imej untuk digunakan sebagai pelindung objek.
Open File Ctrl+F	Membuka fail .txt untuk disembunyikan.
Save As Image Ctrl+S	Menyimpan imej yang telah mengandungi data tersembunyi.
Instructions F1	Pautan ke antaramuka bantuan.

About F2	Pautan ke antaramuka mengenai sistem *steganography*.
	Membuka imej untuk digunakan sebagai pelindung objek.
	Menyimpan imej yang telah mengandungi data tersembunyi.
	Membuka fail .txt untuk disembunyikan.
	Pautan ke antaramuka bantuan.
Hide	Proses penyembunyian data dilakukan.
Extract	Proses pemisahan data dilakukan.
Exit	Keluar daripada sistem *steganography*.

Jadual 6.2 : Fungsi-fungsi utama selain menu dan butang pada antaramuka utama.

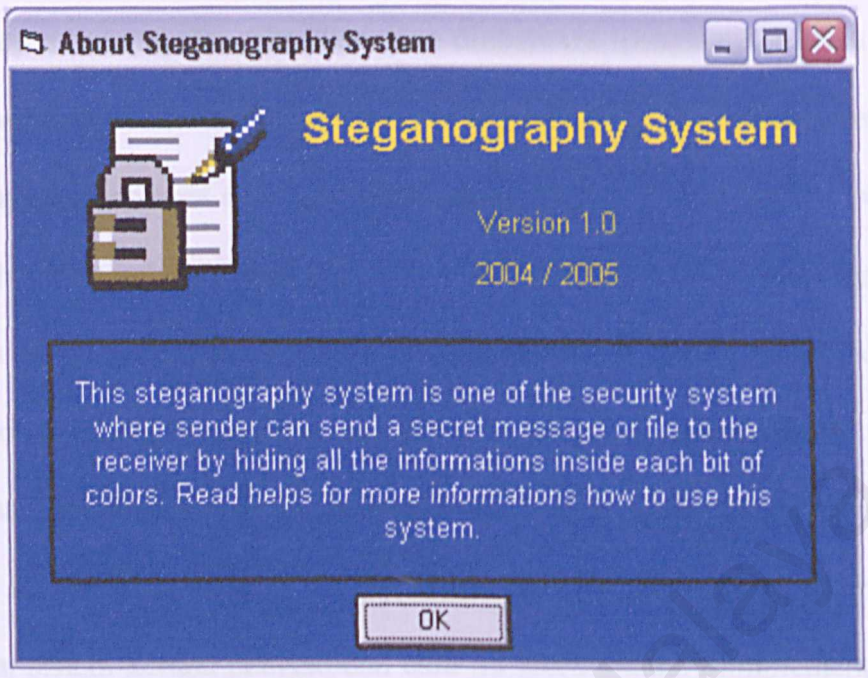
Nombor	Fungsi Utama
1	Lokasi imej bitmap akan dipaparkan.
2	Nama fail .txt akan dipaparkan.
3	Ruangan mesej teks yang ingin disembunyikan.
4	Ruangan kata laluan yang dimasukkan.
5	Imej bitmap akan dipaparkan mengikut saiz imej.

6.2.2 ANTARAMUKA BANTUAN



Rajah 6.2 : Antaramuka bantuan yang disediakan untuk menerangkan bagaimana sistem dapat berfungsi dengan baik.

6.2.3 ANTARAMUKA MENGENAI SISTEM STEGANOGRAPHY



Rajah 6.3 : Antaramuka mengenai Sistem *Steganography*.

6.2.4 PAUTAN ANTARA ANTARAMUKA

Terdapat tiga antaramuka dihasilkan bagi sistem *steganography* ini, iaitu :-

- Antaramuka utama
- Antaramuka bantuan
- Antaramuka mengenai sistem *steganography*

Ketiga-tiga antaramuka ini mempunyai pautan antara satu sama lain. Pautan dilakukan pada antaramuka utama di mana memudahkan pengguna untuk menggunakannya.

6.3 PENGEKODAN

Selepas antaramuka dihasilkan dan diubahsuai, pengekodan perlu dilakukan bagi memastikan sistem dapat berfungsi dengan sebaiknya mengikut keperluan yang telah ditetapkan. Terdapat dua cara pengekodan dilakukan iaitu melalui pengekodan atas bawah atau melalui pengekodan bawah atas. Pengekodan atas bawah ialah melakukan pengekodan aturcara pada modul peringkat tinggi dahulu dan diikuti dengan modul peringkat rendah. Pengekodan bawah atas pula ialah melakukan pengekodan aturcara pada modul peringkat rendah dahulu dan diikuti dengan modul peringkat tinggi. Pengekodan bawah atas menjadi pilihan utama bagi setiap pembangun sistem kerana pengekodan cara ini lebih mudah diimplementasikan dan mengesan ralat yang wujud.

Bagi sistem *steganography*, kedua-dua cara ini akan digunakan bagi memastikan setiap fungsi dapat berfungsi dengan baik dan sistem mengikuti segala keperluan yang telah ditetapkan. Pengekodan akan dilakukan pada peringkat yang lebih mudah dahulu seperti fungsi membuka imej, menyimpan imej, membuka fail dan sebagainya. Kemudian, pengekodan akan dilakukan pada fungsi yang lebih komplek seperti fungsi penyembunyian dan pemisahan data.

Pengekodan aturcara adalah proses yang amat penting bagi membenarkan sistem dapat berfungsi seperti apa yang dikehendaki. Aturcara atau kod yang digunakan dan diaplikasikan adalah tidak terlalu komplek agar penyelenggaraan mudah dilakukan dan untuk pemahaman pembangun itu sendiri. Contoh pengekodan aturcara bagi sistem *steganography* ialah pada Apendiks A.

BAB 7
PENGUJIAN SISTEM

BAB 7

PENGUJIAN SISTEM

7.1 PENGENALAN

Pengujian sistem adalah fasa yang paling penting dalam setiap pembangunan sistem. Pengujian terdiri daripada satu siri langkah-langkah penting yang dapat membantu menentukan kualiti sistem. Pengujian sistem ini dilakukan pada keseluruhan fasa dan bukan sahaja dilakukan pada akhir fasa iaitu selepas sistem telah siap dibangunkan. Setiap aturcara yang dikodkan akan diuji bagi memastikan dan mengesahkan aturcara tersebut berfungsi mengikut keperluan yang telah ditetapkan. Selain itu, pengujian sistem penting dalam menguji keberkesanan sesuatu fungsi yang telah dikodkan dan diaplikasikan.

Pengujian ini dilakukan secara berterusan demi memastikan sistem yang dibangunkan ini menepati objektif sebenar sistem *steganography*. Ini penting agar kualiti sistem *steganography* sentiasa berada pada tahap yang sama dan menepati keperluan fungsian dan keperluan bukan fungsian sistem. Selain itu, pengujian sistem ini dilakukan bagi mendemonstrasi persembahan aturcara dan sistem yang dibangunkan sebelum dipersembahkan kepada pengguna.

Tujuan utama fasa ini dilakukan ialah untuk mengesan kesilapan atau ralat, mengesan kegagalan dan membaiki kesilapan atau ralat yang timbul seperti ralat algoritma, ralat koordinasi dan ralat ketepatan. Matlamat pengujian sistem akan tercapai apabila menemui kesilapan atau ralat serta kegagalan.

Dua perkara utama dalam pengujian sistem ialah :-

- mengenalpasti ralat – menentukan dan mengenalpasti ralat yang menyebabkan sistem gagal berfungsi.
- pembetulan ralat – mengubahsuai sistem atau aturcara yang menghapuskan ralat tersebut.

7.2 JENIS-JENIS RALAT

Terdapat pelbagai ralat yang perlu diambil kira dalam setiap sistem yang dibangunkan. Ralat-ralat ini perlu diketahui agar setiap ralat dapat dikenal pasti dengan lebih cepat dan dapat diselenggara dengan baik. Ini penting agar sistem yang dibangunkan dapat dihindari dengan pelbagai ralat. Ralat-ralat tersebut ialah :-

- ralat algoritma
- ralat sintaks
- ralat dokumentasi
- ralat kompil
- ralat larian
- ralat logik

7.2.1 RALAT ALGORITMA

Ralat algoritma berlaku apabila aturcara logik tidak menghasilkan keputusan atau output yang sebenar bagi input yang dimasukkan. Ralat ini mudah untuk dikesan membaca aturcara sepintas lalu (*desk checking*) atau memeriksa setiap baris aturcara satu persatu.

7.2.2 RALAT SINTAKS

Ralat sintaks berlaku semasa menghuraikan ralat algoritma. Pembangun sistem haruslah menggunakan bahasa pengaturcaraan yang betul bagi mengelakkan berlakunya ralat sintaks. Pembangun haruslah mengetahui struktur setiap bahasa pengaturcaraan yang digunakan. Ini penting bagi mengelakkan ralat sintaks berlaku lagi pada modul atau unit sistem yang lain. Jenis kesilapan dan lokasi ralat akan dipaparkan sebaik sahaja pembangun mengkompil aturcara sistem.

7.2.3 RALAT DOKUMENTASI

Ralat dokumentasi berlaku pula disebabkan dokumentasi yang dihasilkan tidak sepadan atau bersamaan dengan apa yang sepatutnya aturcara berfungsi. Ralat dokumentasi boleh mendorong berlakunya ralat yang lain kerana implementasi sistem yang salah. Ini terhasil disebabkan kesalahan ejaan atau istilah yang digunakan pada sistem yang akan menyebabkan sesuatu pemahaman itu akan berkurang terutama kepada mereka baru membaca dan menggunakan sistem. Kebiasaanya, dokumentasi dihasilkan pada fasa rekabentuk dan perlaksanaan sistem di mana kedua-dua fasa ini menerangkan secara terperinci mengenai sistem terutama pada aturcara dan antaramuka sistem. Antara ralat dokumentasi ialah :-

- ralat pengiraan dan ketepatan
  - formula yang digunakan tidak tepat atau salah.
- ralat kapasiti
  - input yang dimasukkan melebihi had julat yang telah ditetapkan.

- ralat masa atau koordinasi
  - berlaku disebabkan koordinasi kod yang tidak mencukupi.
- ralat persembahan
  - sistem tidak menunjukkan tahap prestasi persembahan sistem yang sebenarnya.

7.2.4 RALAT KOMPIL

Ralat yang dihasilkan dari binaan kod aturcara yang tidak tepat atau salah. Biasanya, ralat kompil ini dapat dikesan ketika proses pengkompilan aturcara atau apabila aturcara dilarikan pada *Visual Basic 6.0*. Setiap ralat kompil yang dijumpai boleh dibaiki dengan mengubahsuai semula kod aturcara yang tidak tepat atau salah.

7.2.5 RALAT LARIAN

Ralat ini berlaku apabila kod aturcara yang digunakan cuba untuk melakukan operasi yang tidak wujud dalam aturcara. Ralat ini boleh dibaiki dengan mengubahsuai kod aturcara semula.

7.2.6 RALAT LOGIK

Ralat seperti ini berlaku apabila kod aturcara yang digunakan tidak melakukan fungsi tertentu sebagaimana yang dikehendaki oleh pembangun sistem. Ralat ini sukar untuk dikesan di mana pembangun haruslah melakukan beberapa

ujian ke atas sistem untuk memastikan kod aturcara melakukan fungsi yang dikehendaki.

7.3 PENGUJIAN

Tiga ujian dilakukan ke atas sistem *steganography* bagi memastikan sistem berada pada tahap kualiti yang memuaskan, iaitu :-

- Pengujian unit
- Pengujian integrasi
- Pengujian sistem

7.3.1 PENGUJIAN UNIT

Pengujian unit adalah pengujian yang pertama di lakukan di mana pengujian dilakukan secara peringkat demi peringkat bermula pada pengekodan aturcara. Pengujian ini dilakukan bagi mengesahkan kod-kod aturcara yang digunakan menghasilkan fungsi seperti yang dikehendaki. Selain itu, ketepatan logik pada setiap aturcara juga akan diuji. Satu persatu unit akan diuji dari peringkat awal hingga ke peringkat akhir. Setiap kesalahan yang dijumpai pada sesuatu unit akan dibetulkan dan diubahsuai dengan serta merta agar tidak timbul masalah lain pada unit yang berlainan. Cara-cara melakukan pengujian unit ialah :-

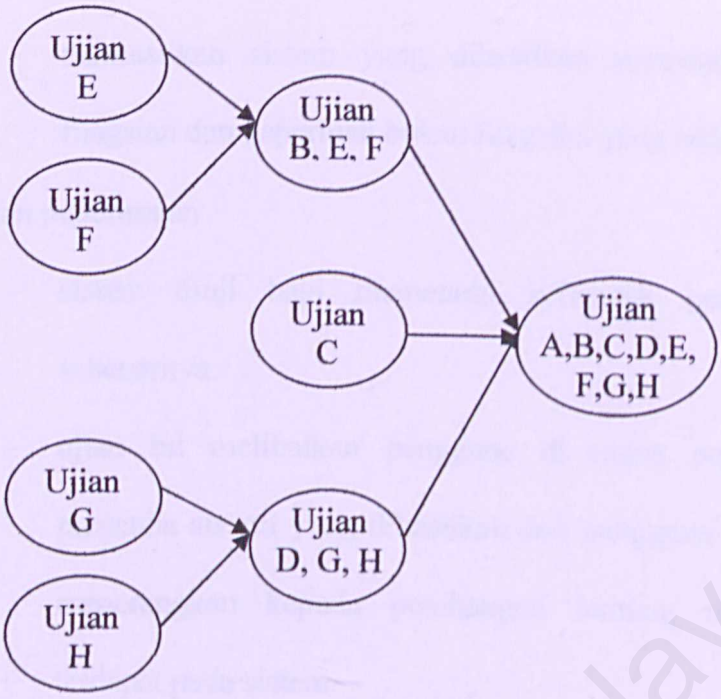
- Melakukan pemeriksaan kod pada setiap unit.
- Menguji komponen aturcara agar output yang sebenar dapat dihasilkan.

- Kod aturcara dilarikan dalam perisian *Microsoft Visual Basic 6.0* untuk mengenalpasti kesalahan.

7.3.2 PENGUJIAN INTEGRASI

Pengujian integrasi pula dilakukan bagi memastikan setiap unit yang digabungkan dapat bekerjasama dengan baik. Setiap unit yang telah diuji akan digabungkan bagi membentuk sistem yang dapat berfungsi. Selain itu, pengujian integrasi juga dilakukan bagi memastikan setiap antaramuka yang dibina pada sistem dapat berkomunikasi dengan baik pada unit-unit yang digabungkan. Disamping itu juga, pengujian unit dilakukan untuk mengesahkan fungsi agar setiap unit-unit melakukan kerja yang telah ditetapkan.

Bagi pengujian unit ini, cara bawah atas digunakan di mana unit-unit atau modul-modul di bahagian bawah akan diuji terlebih dahulu sehingga unit-unit atau modul-modul di bahagian atas. Cara bawah atas dipilih kerana cara ini lebih senang mengesan sebarang masalah, kesilapan, ralat atau kegagalan yang terdapat pada setiap unit. Penyelenggaraan juga mudah dilakukan bagi membetulkan semula unit yang terdapat masalah, kesilapan, ralat atau kegagalan.



Rajah 7.1 : Model bawah atas

7.3.3 PENGUJIAN SISTEM

Pengujian sistem ialah ujian yang dilakukan ke atas keseluruhan sistem yang telah siap dibangunkan. Pengujian ini penting agar sistem dapat beroperasi dengan baik termasuklah unit-unit yang digabungkan, antaramuka-antaramuka sistem dan keseluruhan fungsi secara terperinci. Setiap modul-modul sistem termasuklah modul-modul kecil haruslah dapat berfungsi dengan baik tanpa sebarang masalah. Ini penting bagi memastikan objektif sebenar sistem dipenuhi yang telah dinyatakan pada fasa awal. Selain itu, kualiti sistem dapat dikekalkan sepenuhnya. Terdapat beberapa ujian yang dilakukan dalam pengujian sistem ini, iaitu :-

- Ujian persembahan
  - memastikan sistem yang dihasilkan memenuhi keperluan fungsian dan keperluan bukan fungsian yang telah dinyatakan.
- Ujian penerimaan
  - sistem diuji bagi memenuhi kehendak pengguna yang sebenarnya.
  - ujian ini melibatkan pengguna di mana pengguna akan mencuba sistem yang dihasilkan dan pengguna tersebut akan menerangkan kepada pembangun tentang masalah yang terdapat pada sistem.
- Ujian keselamatan
  - memastikan sistem dilengkapi dengan keperluan keselamatan seperti kata laluan.
- Ujian masa
  - sistem akan diuji dari segi masa tndak balas dan masa larian. Input yang digunakan adalah terdiri daripada pelbagai kategori input bagi menguji masa tindak balas dan masa larian.

7.4 KEPUTUSAN PENGUJIAN

Daripada pengujian yang dijalankan ke atas sistem *steganography* melalui ketiga-tiga pengujian, terdapat beberapa ralat, kesilapan atau kegagalan pada setiap pengujian. Berikut adalah keputusan yang didapati :-

1. Pengujian Unit
    - wujudnya beberapa ralat kecil yang boleh diubahsuai dalam masa yang sama seperti
        - pengisytiharaan yang salah
        - kesilapan pada gelung yang digunakan
        - kesilapan bahasa pengaturcaraan

2. Pengujian Integrasi
    - gabungan unit-unit yang telah diuji terlebih dahulu pada pengujian yang pertama turut menimbulkan ralat seperti
        - masalah memanggil unit atau fungsi
        - antaramuka yang tidak sesuai dengan unit yang digunakan dan terpaksa diubahsuai semula
        - terdapat unit yang tidak berfungsi dengan baik
        - penambahan perpustakaan secara manual ke atas sistem

3. Pengujian Sistem

- sistem diuji bagi menguji tahap keberkesanan sistem dan menepati kehendak objektif dan keperluan pengguna.
- bagi ujian persembahan, sistem yang dihasilkan menepati segala keperluan fungsian dan keperluan bukan fungsian.
- bagi ujian penerimaan, dua pelajar telah dipilih untuk melakukan pengujian penerimaan ke atas sistem dan masalah yang timbul dapat diatasi dengan segera.

BAB 8
PENILAIAN SISTEM

BAB 8

PENILAIAN SISTEM

8.1 PENGENALAN

Fasa yang terakhir dalam pembangunan sistem *steganography* ialah penilaian sistem di mana sistem akan dinilai mengikut beberapa kriteria yang ditetapkan. Sistem akan dinilai apabila keseluruhan sistem telah siap dibangunkan dan boleh digunakan oleh pengguna yang memerlukannya. Sistem *steganography* akan dinilai dari segi :-

- kekuatan sistem
- kekangan atau had sistem
- perancangan masa hadapan sistem

Dalam fasa ini juga, segala masalah dan penyelesaian yang dihadapi oleh pembangun sistem serta cadangan akan dinyatakan.

8.2 KEKUATAN SISTEM

Terdapat beberapa kekuatan pada sistem *steganography*. Kekuatan sistem steganography ini penting bagi memastikan sistem steganography yang dibangunkan mempunyai kualiti yang tersendiri. Kekuatan-kekuatan tersebut ialah :-

1. **Mudah dibawa ke mana-mana.**

   Sistem *steganography* yang dibangunkan mempunyai saiz yang kecil di mana pengguna boleh membawanya ke mana-mana apabila diperlukan. Pengguna juga boleh menyimpan sistem *steganography* ini di dalam peranti luaran seperti disket, cakera padat dan *thumb drive* untuk dibawa ke mana-mana. Ini akan memudahkan pengguna yang menggunakan komputer yang berlainan.

2. **Kata laluan yang berbeza.**

   Pengguna yang menggunakan sistem ini boleh menggunakan kata laluan yang berbeza. Kata laluan adalah tidak tetap seperti mana pengguna perlu mendaftar terlebih dahulu. Pengguna boleh menggunakan kata laluan yang berbeza untuk menyembunyikan teks atau fail dan dihantar pada pengguna lain yang berlainan. Ini memberi kelebihan kepada pengguna di mana tidak perlu mengingati kata laluan setiap kali hendak melakukan proses penyembunyian teks atau fail.

3. **Mesra pengguna.**

Sistem yang dihasilkan adalah mesra pengguna di mana hanya dua butang utama pada antaramuka utama iaitu butang penyembunyian data dan butang pemisahan data. Ikon-ikon lain yang digunakan di dalam sistem adalah sama dengan ikon-ikon yang terdapat pada perisian-perisian lain yang juga turut mempunyai fungsi yang sama. Ini akan dapat memudahkan lagi pemahaman pengguna. Bantuan dan keterangan secara terperinci juga terdapat pada sistem yang dapat membantu pengguna memahami proses-proses utama sistem.

4. **Paparan peringatan.**

Sistem *steganography* dapat memaparkan mesej peringatan kepada pengguna setiap kali pengguna melakukan kesilapan ketika menggunakan sistem ini. Ini penting supaya output atau keputusan yang dihasilkan adalah seperti apa yang dikehendaki.

5. **Dua pilihan utama.**

Terdapat dua pilihan utama di mana pengguna boleh memilih samada ingin menyembunyikan teks atau fail disebalik pelindung objek (imej bitmap).

8.3 KEKANGAN ATAU HAD SISTEM

Walaupun sistem *steganography* mempunyai beberapa kekuatan sistem, terdapat juga kekangan atau had sistem pada sistem *steganography*. Kekangan atau had tersebut ialah :-

1. Imej yang digunakan sebagai pelindung objek hanyalah imej yang berformat bitmap 24-bit sahaja.

2. Fail yang digunakan untuk disembunyikan hanyalah fail berformat teks iaitu .txt.

3. Fail teks yang mengandungi jumlah perkataan yang besar dan saiz fail yang besar akan menyebabkan masa tindak balas sistem menjadi lambat. Ini kerana, setiap huruf akan disembunyikan pada setiap bit imej.

4. Saiz imej bitmap 24-bit yang digunakan sebagai pelindung objek tidak boleh melebihi 1 MB bagi mengelakkan proses penghantaran emel menjadi lambat.

5. Teks yang hendak disembunyikan adalah terhad sebanyak 2000 huruf.

6. Sistem *steganography* yang dibangunkan adalah bukan untuk jangka masa yang panjang.

7. Hanya pengguna yang mempunyai sistem yang seumpama dengan sistem *steganography* boleh membaca teks atau fail yang disembunyikan disebalik imej.

8.4 PERANCANGAN MASA HADAPAN SISTEM

Terdapat lima perancangan masa hadapan bagi sistem *steganography* iaitu :-

1. Mengaplikasikan proses kriptografi pada mesej teks atau fail yang hendak disembunyikan. Ini akan menambahkan lagi keselematan data yang dihantar di mana proses kriptografi dan *steganography* akan dilakukan pada satu sistem yang sama.

2. Imej yang digunakan sebagai pelindung objek adalah tidak terhad pada satu format sahaja. Imej-imej yang berformat lain seperti JPEG, GIF dan sebagainya.

3. Fail yang hendak disembunyikan tidak terhad pada format teks (.txt.) sahaja. Fail yang berformat lain juga boleh digunakan untuk disembunyikan.

4. Teks tidak terhad pada 2000 huruf sahaja. Ini akan dapat memberi peluang kepada pengguna untuk menggunakan jumlah teks yang banyak tetapi jumlah teks tersebut mestilah dihadkan pada satu tahap.

8.5 MASALAH DAN PENYELESAIAN

Dalam membangunkan sistem *steganography* ini, terdapat pelbagai masalah yang dihadapi samada sebelum, ketika atau selepas sistem dibangunkan. Walau bagaimanapun, setiap masalah yang dihadapi dapat diatasi dengan segera agar tidak timbul masalah yang berpanjangan. Berikut adalah masalah-masalah yang dihadapi :-

Masalah 1

Ketika sistem hendak dibangunkan, terdapat masalah dalam mencari perkakasan dan perisian yang sesuai. Ini kerana, setiap perkakasan dan perisian mempunyai ciri-ciri yang tertentu dan kelebihan yang tersendiri. Terdapat pelbagai perisian yang boleh dibandingkan pada masa kini, sehingga tidak dapat membuat keputusan yang bijak dalam menentukan perisian mana yang sesuai untuk membangunkan sistem *steganography*. Masalah ini juga timbul dalam menentukan perkakasan yang sesuai.

Penyelesaian

Dalam menentukan perkakasan dan perisian yang sesuai, pelbagai maklumat dirujuk agar perkakasan dan perisian yang dipilih dapat menghasilkan sistem yang dikehendaki. Maklumat dikumpul dengan pelbagai cara iaitu melalui internet, buku-buku yang berkenaan dan melalui pertanyaan daripada orang yang berpengalaman. Setiap maklumat yang didapati akan dianalisa dan difahami agar tidak tersilap dalam membuat keputusan. Selepas analisa dan pemahaman dibuat ke atas maklumat yang didapati, *Microsoft Visual Basic 6.0* menjadi pilihan utama dalam membangunkan sistem *steganography*. Selain itu, perkakasan yang bersesuaian dengan perisian yang dipilih juga digunakan.

Masalah 2

Perisian yang dipilih iaitu *Microsoft Visual Basic 6.0* adalah perisian yang tidak pernah digunakan sebelum ini. Ini mendatangkan masalah terutama sekali ketika hendak membangunkan sistem pada fasa awal. Masalah ini termasuklah bagaimana perisian ini berfungsi, bahasa pengaturcaraan yang digunakan dan juga mengendalikan perisian ini dengan baik.

Penyelesaian

Bagi memahami perisian *Microsoft Visual Basic 6.0*, pelbagai rujukan dan kajian dilakukan. Sumber utama rujukan ialah pada buku *Microsoft Visual Basic 6.0*. Selain itu, rujukan juga dibuat melalui internet di mana hampir 40 peratus pembelajaran melalui internet. Ini kerana, jumlah buku yang digunakan adalah terhad berbanding maklumat yang didapati daripada internet. Terdapat juga bantuan yang diberikan oleh rakan-rakan yang mahir dalam menggunakan *Microsoft Visual Basic 6.0*.

Masalah 3

Kemudahan komputer yang tidak mencukupi di mana pelajar terpaksa berkongsi komputer di makmal tesis untuk menyiapkan tesis dan tugasan masing-masing. Setiap komputer terpaksa dikongsi oleh beberapa orang pelajar dan kadang-kadang setiap pelajar menggunakan perisian yang berlainan. Ini telah menyebabkan berlakunya pertembungan masa antara pelajar kerana setiap pelajar mahu menyiapkan projek mereka dalam masa yang telah ditetapkan.

Penyelesaian

Bagi memudahkan sistem *steganography* dibangunkan tanpa berlakunya pertembungan dengan pelajar lain, saya membuat keputusan untuk menggunakan komputer sendiri di kolej kediaman. Walau bagaimanapun, saya masih lagi menggunakan komputer di makmal dalam meneruskan kajian mengenai sistem yang dibangunkan melalui internet dan juga menyiapkan laporan projek.

8.6 CADANGAN

Terdapat beberapa cadangan yang ingin dikemukakan bagi melancarkan proses pembangunan sistem kepada pelajar-pelajar lain pada masa akan datang. Antaranya ialah :-

1. Mengadakan kursus atau seminar yang berkaitan dengan penggunaan *Microsoft Visual Basic 6.0* di mana dapat membantu para pelajar yang ingin menggunakan perisian ini dalam membangunkan sistem mereka. Ini kerana, kebanyakan pelajar kurang mahir dalam menggunakan perisian ini berbanding perisian-perisian lain. Pelajar-pelajar yang berada pada tahun pertama dan kedua juga boleh menyertainya sebagai persediaan pada tahun hadapan.

2. Mempelbagaikan dan memperbanyakkan kemudahan komputer di fakulti untuk digunakan oleh pelajar agar tidak ada berlakunya pertembungan dalam menggunakan komputer.

3. Menetapkan setiap pelajar yang mengambil kursus WXES 3181 dan WXES 3182 mesti berjumpa dengan penyelia atau moderator sekurang-kurangnya sekali dalam dua minggu. Ini bagi memastikan projek yang dibangunkan berada pada laluan yang betul.

APENDIKS A

CONTOH SEBAHAGIAN PENGEKODAN FUNGSI

1. Pembukaan imej bitmap :-

```
Private Sub mnuOpenImage_Click()

Dim sFileName As String
Dim sPicture As Single
Dim sName As String

With CD1
   .DialogTitle = "Open image"
   .flags = cdlOFNFileMustExist Or cdlOFNHideReadOnly Or cdlOFNLongNames
   .Filter = "Windows Bitmap (*.bmp)|*.bmp"
   .ShowOpen
   sFileName = .FileName
End With

If sFileName <> "" Then
   Pic1.Picture = LoadPicture(sFileName)
   imgLoaded = True
   arrangeControls
   DPicture.Text = CD1.FileName
   sName = CD1.FileTitle
   sPicture = FileLen(sFileName)

   While sPicture > 1024 ^ 2 Or sPicture < 0
      MsgBox ("File Name : " & sName + Chr$(13) + "Size of File : " &
      FormatBytes(CLng(sPicture))), vbInformation + vbOKOnly, "Image File"
      ReturnValue = MsgBox("The picture is too large! Please load the new picture.", 53,
     "Warning")
      If (ReturnValue = 4) Then
         CD1.DialogTitle = "Open image"
         CD1.flags = cdlOFNFileMustExist Or cdlOFNHideReadOnly Or
         cdlOFNLongNames
         CD1.Filter = "Windows Bitmap (*.bmp)|*.bmp"
         CD1.ShowOpen
         sFileName = CD1.FileName

            If sFileName <> "" Then
               Pic1.Picture = LoadPicture(sFileName)
               imgLoaded = True
               arrangeControls
               DPicture.Text = CD1.FileName
               sPicture = FileLen(sFileName)
            End If
      Else

         End

      End If
   Wend
```

```
        If sPicture = 1024 ^ 2 Then
            MsgBox ("File Name : " & sName + Chr$(13) + "Size of File : " &
            FormatBytes(CLng(sPicture))), vbInformation + vbOKOnly, "Image File"
            cmdEncode.Enabled = True
            cmdDecode.Enabled = True
        Else
            If sPicture < 1024 ^ 2 Then
                MsgBox ("File Name : " & sName + Chr$(13) + "Size of File : " &
                FormatBytes(CLng(sPicture))), vbInformation + vbOKOnly, "Image File"
                cmdEncode.Enabled = True
                cmdDecode.Enabled = True
            Else
                MsgBox ("File Name : " & sName + Chr$(13) + "Size of File : " & sPicture & "
                KB"), vbInformation + vbOKOnly, "Image File"
                cmdEncode.Enabled = True
                cmdDecode.Enabled = True
            End If
        End If

End If

With CD1
    .InitDir = CD1.FileName
    .FileName = CD1.FileTitle
End With
End Sub
```

2. Penyimpanan imej

```
Private Sub mnuSaveAs_Click()

Dim sFileName As String

With CD1

    .DialogTitle = "Save image"
    .flags = cdlOFNOverwritePrompt Or cdlOFNHideReadOnly Or cdlOFNLongNames
    .Filter = "Windows Bitmap (*.bmp)|*.bmp"
    .FileName = ""
    .DefaultExt = ".bmp"
    .ShowSave
    sFileName = .FileName

    If sFileName <> "" Then
        SavePicture Pic1.Picture, sFileName
    End If

    .InitDir = CD1.FileName
    .FileName = CD1.FileTitle

End With

End Sub
```

3. Pembukaan Fail

```
Private Sub mnuOpenFile_Click()

Dim sFileName As String
Dim sFile As Single

With CD1
   .DialogTitle = "Open file"
   .flags = cdlOFNFileMustExist Or cdlOFNHideReadOnly Or cdlOFNLongNames
   .Filter = "Text Files (*.txt)|*.txt"
   .FileName = ""
   .ShowOpen
   sFileName = .FileName
End With

If sFileName <> "" Then
   sFile = FileLen(sFileName)
   DFile.Text = CD1.FileTitle

   While sFile > FileLen(DPicture.Text)
   ReturnValue = MsgBox("The file is bigger than image you have loaded!.", 53, "Warning")
      If (ReturnValue = 4) Then
         CD1.DialogTitle = "Open file"
         CD1.flags = cdlOFNFileMustExist Or cdlOFNHideReadOnly Or
         cdlOFNLongNames
         CD1.Filter = "Text Files (*.txt)|*.txt"
         CD1.ShowOpen
         DFile.Text = CD1.FileName
         sFile = FileLen(DFile.Text)
      Else
         End
      End If
   Wend
End If

End Sub
```

4. Proses penyembunyian teks dan fail dilakukan

```
Private Sub cmdEncode_Click()

Dim msg As String
Dim strFile As String
Dim fName As String
Dim fLen As Long
Dim i As Long
Dim Used_Positions As Collection
Dim ImgWidth As Integer
Dim ImgHeight As Integer
Dim fref1 As Long
```

```
Screen.MousePointer = vbHourglass
DoEvents

Rnd -1
Randomize NumericPassword(Password.Text)

If Option2.Value = True Then
   If Len(Message1.Text) = 0 Then
      MsgBox ("Please insert your text first!"), vbCritical + vbOKOnly, "Error"
      Password.Text = ""
   Else
      ImgWidth = Pic1.ScaleWidth
      ImgHeight = Pic1.ScaleHeight
      msg = Left$(Message1.Text, Len(Message1.Text))
      Set Used_Positions = New Collection

      EncodeByte Len(msg), _
         Used_Positions, ImgWidth, ImgHeight

      For i = 1 To Len(msg)
         EncodeByte Asc(Mid$(msg, i, 1)), _
            Used_Positions, ImgWidth, ImgHeight
      Next i

      Message1.Text = ""

      Pic1.Picture = Pic1.Image
      MsgBox ("Your message or file was Hidden!"), vbInformation + vbOKOnly, "Hidden"
      Password.Text = ""
      Screen.MousePointer = vbDefault
   End If
End If

If Option1.Value = True Then
   If Len(DFile.Text) = 0 Then
      MsgBox ("Please insert your file.txt first!"), vbCritical + vbOKOnly, "Error"
      Password.Text = ""
   Else
      fLen = FileLen(DFile.Text)
      fref1 = FreeFile

      Open DFile.Text For Binary Access Read As #fref1

      DFile.Text = Input$(fLen, fref1)

      ImgWidth = Pic1.ScaleWidth
      ImgHeight = Pic1.ScaleHeight
      fName = Left$(DFile.Text, fLen)
      Set Used_Positions = New Collection

      EncodeByte fLen, _
         Used_Positions, ImgWidth, ImgHeight

      For i = 1 To fLen
```

```
        EncodeByte Asc(Mid$(fName, i, 1)), Used_Positions, ImgWidth, ImgHeight
    Next i

    DFile.Text = ""

    Pic1.Picture = Pic1.Image
    MsgBox ("Your message or file was Hidden!"), vbInformation + vbOKOnly, "Hidden"
    Password.Text = ""
    Screen.MousePointer = vbDefault
  End If

End If

Screen.MousePointer = vbDefault
End Sub
```

5. Proses pemisahan data daripada imej

```
Private Sub cmdDecode_Click()

On Error GoTo ErrSub

Dim msg_length As Long
Dim msg As String
Dim ch As Long
Dim i As Integer
Dim Used_Positions As Collection
Dim ImgWidth As Integer
Dim ImgHeight As Integer
Dim fLen As Long
Dim strFile As String
Dim file_length As Long
Dim fref2 As Long
Dim file2save As String
Dim reply As String

Screen.MousePointer = vbHourglass
DoEvents

Rnd -1
Randomize NumericPassword(Password.Text)

If Option2.Value = True Then

  ImgWidth = Pic1.ScaleWidth
  ImgHeight = Pic1.ScaleHeight
  Set Used_Positions = New Collection

  msg_length = DecodeByte(Used_Positions, ImgWidth, ImgHeight)

  For i = 1 To msg_length
    ch = DecodeByte(Used_Positions, ImgWidth, ImgHeight)
    msg = msg & Chr$(ch)
```

```
    Next i

    Pic1.Picture = Pic1.Image
    Message1.Text = msg
  End If

  If Option1.Value = True Then

    file2save = getfile("Text Files (*.txt*)" + Chr$(0) + "*.txt" + Chr$(0), "Save File As ...",
    Me.hWnd, 3)

    While file2save = "Cancel"
    reply = MsgBox("Are you sure to cancel the extraction process?", vbYesNo Or
    vbQuestion, "Steganography System")

    If reply = vbYes Then
    End

    ElseIf reply = vbNo Then
    file2save = getfile("Text Files (*.txt*)" + Chr$(0) + "*.txt" + Chr$(0), "Save File As ...",
    Me.hWnd, 3)

    End If

    Wend

    ImgWidth = Pic1.ScaleWidth
    ImgHeight = Pic1.ScaleHeight
    Set Used_Positions = New Collection

    file_length = DecodeByte(Used_Positions, ImgWidth, ImgHeight)

    For i = 1 To file_length
      ch = DecodeByte(Used_Positions, ImgWidth, ImgHeight)
      msg = msg & Chr$(ch)
    Next i

    Pic1.Picture = Pic1.Image
    fref2 = FreeFile

    Open file2save For Binary As #fref2
    Put #fref2, , msg
    Close #fref2

  End If

  Password.Text = ""
  Screen.MousePointer = vbDefault

  ErrSub:
  If Err.Number <> 0 Then
  MsgBox ("Make sure your PASSWORD is correct!"), vbCritical + vbOKOnly, "Error"
  Screen.MousePointer = vbDefault
  Password.SetFocus
```

```
Exit Sub
End If

End Sub
```

6. Penyimpanan fail

```
Function getfile(Filter As String, title As String, Handle As Long, flags As Long) As String

    Dim ofn As Savefilename
    Dim a

    ofn.lStructSize = Len(ofn)
    ofn.hwndOwner = Handle
    ofn.hInstance = App.hInstance
    ofn.lpstrFilter = Filter
    ofn.lpstrFile = Space$(254)
    ofn.nMaxFile = 255
    ofn.lpstrFileTitle = Space$(254)
    ofn.nMaxFileTitle = 255
    ofn.lpstrInitialDir = App.Path
    ofn.lpstrTitle = title
    ofn.flags = flags
    ofn.lpstrDefExt = ".txt"

    a = GetSaveFileName(ofn)

    If (a) Then
       getfile = Trim$(ofn.lpstrFile)
    Else
       getfile = "Cancel"
    End If
End Function
```

7. Pembesaran imej

```
Private Sub arrangeControls()

Width = Pic1.Left + Pic1.Width + Width - ScaleWidth + 120
Height = Pic1.Top + Pic1.Height + Height - ScaleHeight + 120

End Sub
```

8. Memformat saiz

```
Private Function FormatBytes(ByVal num_bytes As Long) As String

Dim txt As String

    txt = Space$(256)
    StrFormatByteSize num_bytes, txt, Len(txt)
    FormatBytes = Left$(txt, InStr(txt, vbNullChar) - 1)
End Function
```

9. Pautan antara antaramuka

```
Private Sub mnuIns_Click()

helps.Show

End Sub


Private Sub mnuAbout_Click()

about.Show

End Sub
```

10. Antaramuka utama dimuatkan

```
Private Sub Form_Load()

Pic1.ScaleMode = vbPixels
Pic1.AutoRedraw = True
CD1.InitDir = App.Path
arrangeControls
PBar1.Max = 15
mnuOpenFile.Enabled = False
Toolbar1.Buttons("OpenF").Enabled = False

End Sub
```

11. Kata laluan

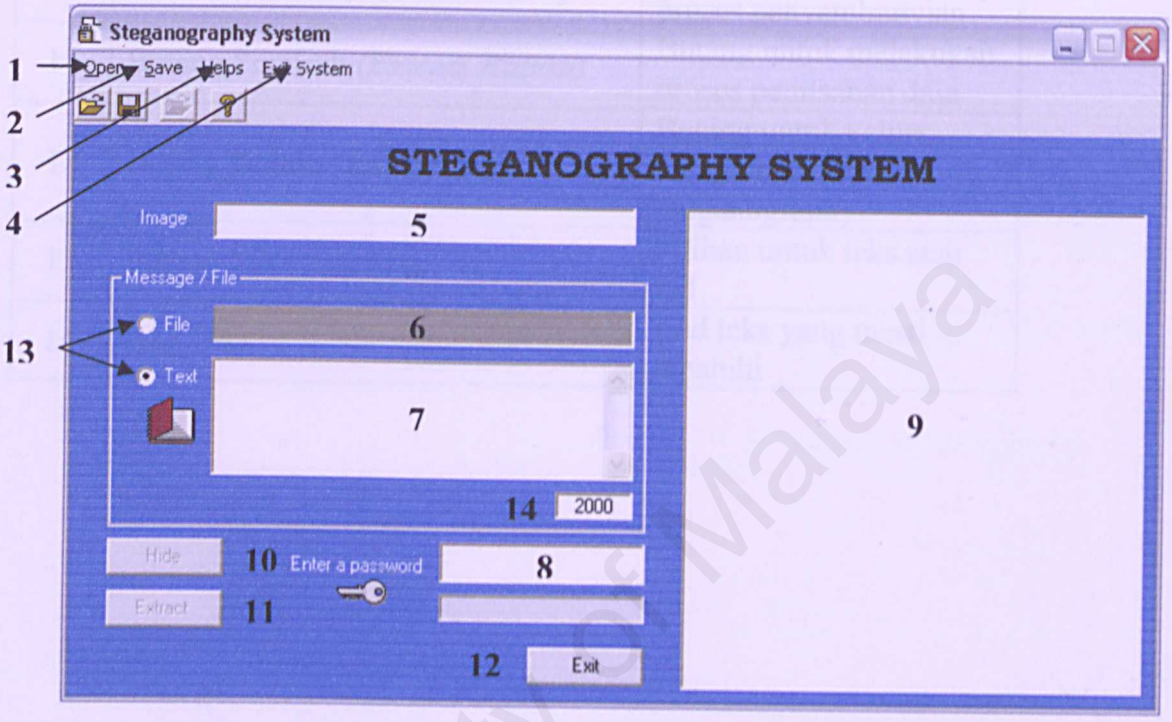
```
Private Function NumericPassword(ByVal Password As String) As Long

Dim Value As Long
Dim ch As Long
Dim shift1 As Long
Dim shift2 As Long
Dim i As Integer
Dim str_len As Integer

shift1 = 3
shift2 = 17
str_len = Len(Password)

For i = 1 To str_len
    ch = Asc(Mid$(Password, i, 1))
    Value = Value Xor (ch * 2 ^ shift1)
    Value = Value Xor (ch * 2 ^ shift2)
    shift1 = (shift1 + 7) Mod 19
    shift2 = (shift2 + 13) Mod 23
Next i
NumericPassword = Value
End Function
```

APENDIKS B

MANUAL PENGGUNA
SISTEM STEGANOGRAPHY

MANUAL PENGGUNA SISTEM STEGANOGRAPHY

1. PENGENALAN



Rajah 1.1 : Antaramuka utama Sistem *Steganography*.

Petunjuk:

No.	Keterangan	Fungsi
1	Menu Buka ***(Open Menu)***	Digunakan untuk membuka fail imej atau fail untuk disembunyikan
2	Menu Simpan ***(Save Menu)***	Digunakan untuk menyimpan imej
3	Menu Bantuan ***(Helps Menu)***	Digunakan untuk
4	Menu Keluar Sistem ***(Exit System Menu)***	Digunakan untuk keluar daripada Sistem Steganography
5	Lokasi fail imej ***(Image File Path)***	Lokasi fail imej akan dipaparkan
6	Kotak Nama Fail ***(File Name Box)***	Nama fail .txt yang dipilih akan dipaparkan

7	Kotak Teks ***(Text Box)***	Ruang untuk memasukkan teks yang dikehendaki
8	Kotak Kata Laluan ***(Password Box)***	Ruang untuk memasukkan kata laluan
9	Kotak Imej ***(Image Box)***	Imej yang dipilih akan dipaparkan
10	Butang Sembunyi ***(Hide Button)***	Butang untuk melakukan proses penyembunyian
11	Butang Pemisah ***(Extract Button)***	Butang untuk melakukan proses pemisahan data
12	Butang Keluar ***(Exit Button)***	Butang untuk keluar daripada Sistem Steganography
13	Pilihan Teks atau Fail	Pilihan untuk teks atau fail
14	Had Teks	Had teks yang mesti dipatuhi

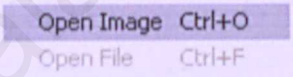
2. CARA MEMASUKI SISTEM

2.1 Klik 2 kali pada ikon 

3. CARA PENYEMBUNYIAN TEKS ATAU FAIL

3.1 Pilih satu imej bitmap (**24 *bitmap image***).

- Klik pada Menu Buka (***Open Menu***). 

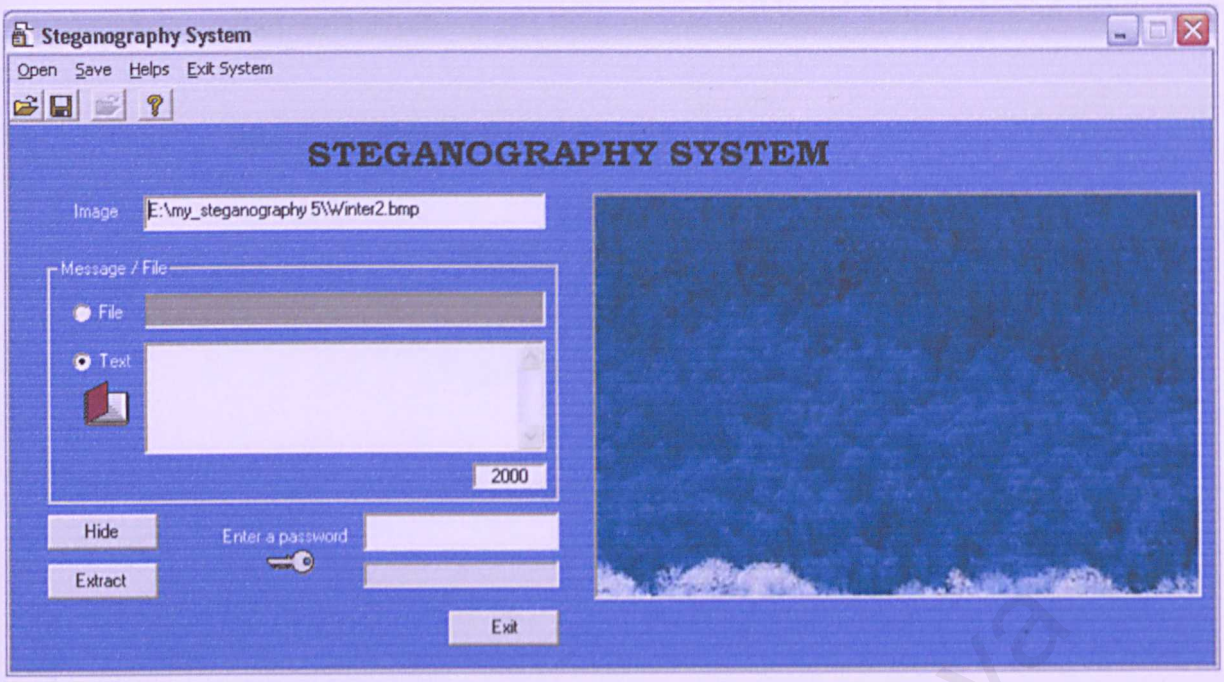
- Pilih Buka Imej (***Open Image***). 

  atau klik pada 

- Cari imej yang hendak digunakan. Imej yang dipilih akan dipaparkan pada bahagian sebelah kanan sistem.

- Imej akan membesar mengikut saiz sebenar imej tersebut seperti Rajah 1.2.

Amaran : Saiz imej mestilah tidak melebihi 1 MB



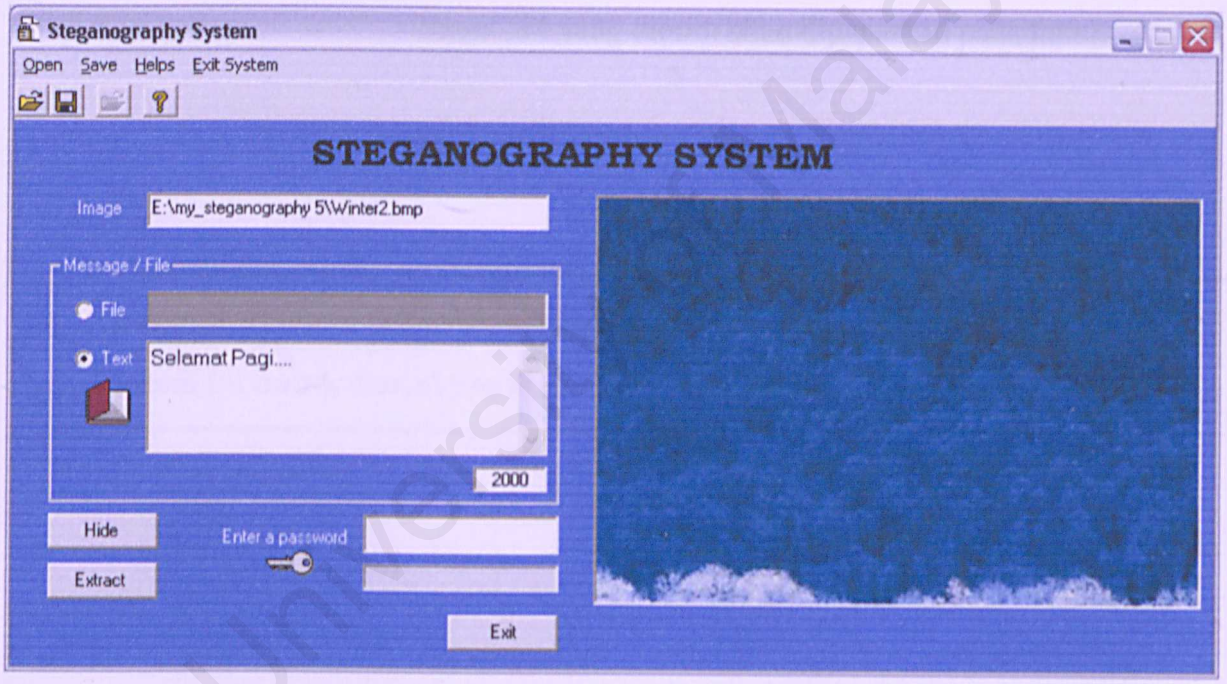
Rajah 3.1 : Sistem *Steganography* selepas imej dibuka.

3.2 Nama dan saiz sebenar imej yang dipilih akan dipaparkan.

Rajah 3.2 : Kotak mesej nama dan saiz imej.

3.3 Jika anda hendak menyembunyikan maklumat yang berbentuk teks mesej (Rajah 3.3) : -

- Pilih pada Pilihan Teks (***Teks Option***).
- Taip teks mesej anda pada Kotak Teks yang disediakan. Teks anda mestilah tidak melebihi 2000 huruf.

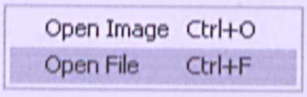


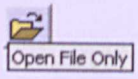
Rajah 3.3 : Pemilihan teks.

3.4 Jika anda hendak menyembunyikan fail (Rajah 3.4) :-

- Pilih pada Pilihan Fail (***File Option***).

- Klik pada Menu Buka (***Open Menu***). 

- Pilih Buka Fail (***Open File***) 

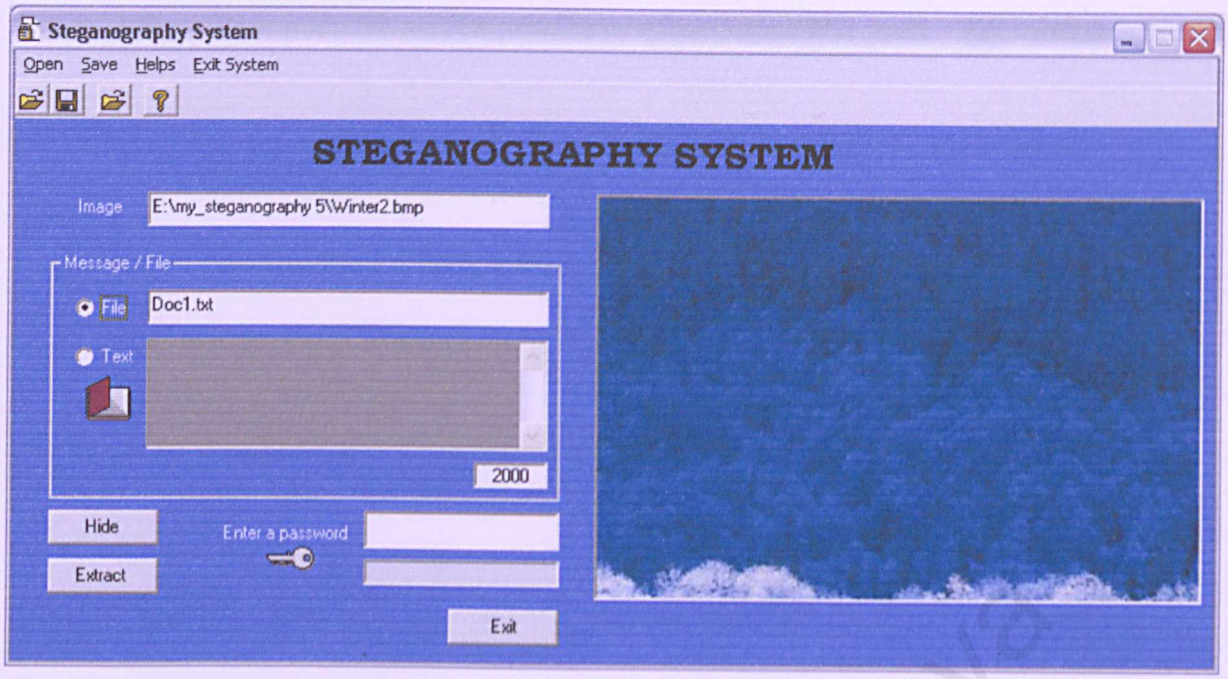
  atau klik pada 

- Cari fail yang anda kehendaki untuk disembunyikan.

- Nama fail yang dipilih akan dipaparkan pada kotak

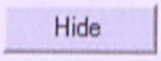
  Nama Fail (***File Name Box***).

Amaran : Hanya fail yang berformat .txt sahaja boleh digunakan dalam sistem ini untuk disembunyikan.

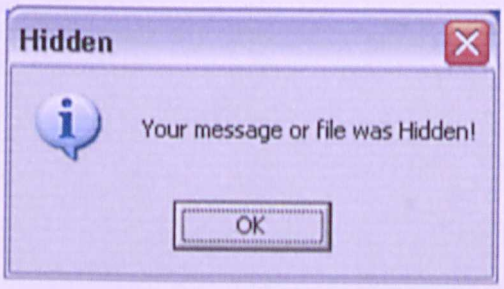


Rajah 3.4 : Pemilihan fail.

3.5 Masukkan kata laluan anda yang tidak melebihi 15 huruf.

3.6 Klik pada Butang Sembunyi (***Hide Button***). 

3.7 " ***Your message or file was hidden*** " akan dipaparkan. Ini bermakna, proses penyembunyian maklumat atau fail telah berjaya.



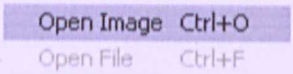
Rajah 3.5 : Kotak mesej proses penyembunyian berjaya dilakukan.

3.8 Klik pada Menu Simpan (***Save Menu***) atau klik pada  untuk menyimpan imej anda yang mengandungi maklumat atau fail tersembunyi sebelum dihantar kepada penerima melalui emel.

4. CARA PEMBACAAN TEKS ATAU FAIL

4.1 Pilih satu imej bitmap (**24 *bitmap image***).

- Klik pada Menu Buka (***Open Menu***). 

- Pilih Buka Imej (***Open Image***) 

atau klik pada 

- Cari imej yang hendak digunakan. Imej yang dipilih akan dipaparkan pada bahagian sebelah kanan sistem.

- Imej akan membesar mengikut saiz sebenar imej tersebut seperti Rajah 3.1.

4.2 Nama dan saiz sebenar imej yang dipilih akan dipaparkan seperti Rajah 3.2.

4.3 Jika teks mesej yang disembunyikan :-

- Pilih pada Pilihan Teks (***Text Option***)

4.4 Jika fail yang disembunyikan :-

- Pilih pada Pilihan Fail (***File Option***)

Secara lalainya, Pilihan Teks (***Text Option***) akan dipilih.

4.5 Masukkan kata laluan yang sama ketika proses penyembunyian maklumat atau fail. Selalunya, kata laluan yang digunakan oleh pengirim.

4.6 Klik pada butang pemisah (***Extract Button***) Extract untuk memisahkan teks mesej atau fail daripada imej.

4.7 Jika teks mesej yang disembunyikan (Rajah 4.1) :-

- Anda boleh membacanya secara terus pada Kotak Teks (***Text Box***).

Rajah 4.1 : Paparan teks setelah proses pemisahan data.

4.8 Jika fail yang disembunyikan :-

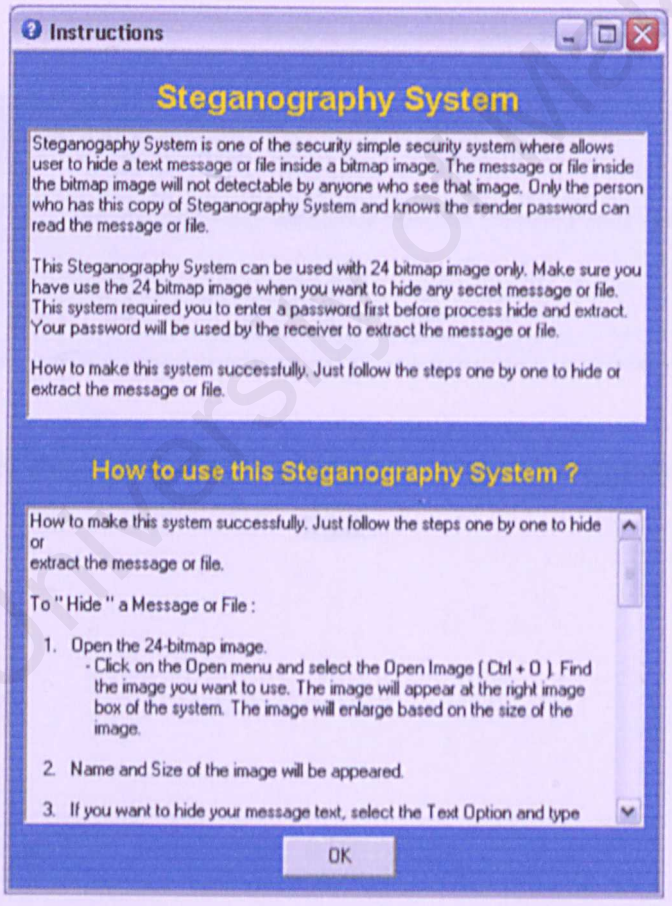
- Anda dikehendaki menyimpan fail tersebut dahulu sebelum membacanya.

- Tetingkap Simpan (***Save Windows***) akan dipaparkan secara automatik selepas anda klik pada butang pemisah (***Extract Button***).

5. CARA MENDAPATKAN BANTUAN

5.1 Klik pada Menu Bantuan (***Helps Menu***) atau klik pada  untuk mendapatkan bantuan menggunakan sistem Steganography.

5.2 Tetingkap Arahan (***Instructions Windows***) akan dipaparkan seperti Rajah 5.1.

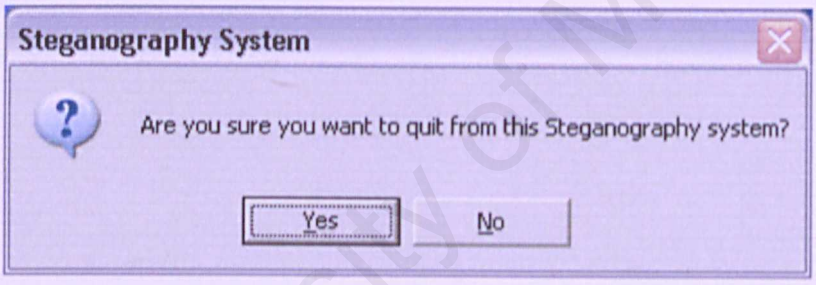


Rajah 5.1 : Tetingkap Arahan (*Instructions Windows*).

6. CARA MENAMATKAN SISTEM

6.1 Klik pada Butang Keluar (***Exit Button***) Exit atau klik pada Menu Keluar Sistem (***Exit System Menu***) untuk keluar daripada sistem ini.

6.2 Klik ***Yes*** untuk keluar terus daripada sistem atau klik ***No*** untuk memasuki semula sistem pada kotak mesej seperti Rajah 6.1.



Rajah 6.1 : Kotak mesej untuk memastikan samada pengguna ingin keluar atau tidak.

RUJUKAN

RUJUKAN

Whitten, J. L., Bentley, L. D. & Dittman, K. C. (2002). *System Analysis and Design Method*. Ed. Ke-6. McGraw-Hill Higher Education.

Raymond, R. P. (2004). *Corporate Computer and Network Security*. Prentice Hall.

Pfleeger, S.L. (1998). *Software Engineering : Theory and Practice*. Prentice Hall.

The Art of Steganography. (n.d). Diperolehi Ogos 8, 2004, dari http://www.sine.org/practical/GSEC/Asha_Patel_GSEC.pdf.

Sellapan, P. (1996). *Visual Basic : A Reference For Beginners & Developers*. Ed. Ke-1. Aneka Publishing

Bride, Mac. (2004). *Visual Basic : Teach Yourself*. Ed. Ke-1. McGraw-Hill.

Mohanty, S.P. (1999). *Journal of Digital Watermarking : A Tutorial Review*. Department of Computer Science and Engineering, University of South Florida.

Cacciaguerra, S. & Ferretti, S. *Journal of Data Hiding : Steganography and Copyright Marking*. Department of Computer Science, University of Bologna.

Provos, N. & Honeyman, P. Hide and Seek : An Introduction To Steganography. University of Michigan.